Red Hat Network Satellite 5.0 Reference Guide

Red Hat Network Satellite
Edition 1

Landmann

Red Hat Network Satellite 5.0 Reference Guide

Red Hat Network Satellite
Edition 1

Landmann
rlandmann@redhat.com

Legal Notice

Copyright © 2007 Red Hat, Inc.

This document is licensed by Red Hat under the Creative Commons Attribution-ShareAlike 3.0 Unported License. If you distribute this document, or a modified version of it, you must provide attribution to Red Hat, Inc. and provide a link to the original. If the document is modified, all Red Hat trademarks must be removed.

Red Hat, as the licensor of this document, waives the right to enforce, and agrees not to assert, Section 4d of CC-BY-SA to the fullest extent permitted by applicable law.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo, JBoss, MetaMatrix, Fedora, the Infinity Logo, and RHCE are trademarks of Red Hat, Inc., registered in the United States and other countries.

Linux ® is the registered trademark of Linus Torvalds in the United States and other countries.

Java ® is a registered trademark of Oracle and/or its affiliates.

XFS ® is a trademark of Silicon Graphics International Corp. or its subsidiaries in the United States and/or other countries.

MySQL ® is a registered trademark of MySQL AB in the United States, the European Union and other countries.

Node.js ® is an official trademark of Joyent. Red Hat Software Collections is not formally related to or endorsed by the official Joyent Node.js open source or commercial project.

The OpenStack ® Word Mark and OpenStack Logo are either registered trademarks/service marks or trademarks/service marks of the OpenStack Foundation, in the United States and other countries and are used with the OpenStack Foundation's permission. We are not affiliated with, endorsed or sponsored by the OpenStack Foundation, or the OpenStack community.

All other trademarks are the property of their respective owners.

Abstract

Welcome to the Red Hat Network 5.0.0 Reference Guide. The RHN Reference Guide guides you through registering systems with Red Hat Network and using its many features.

Table of Contents

Introduction to the Guide **13**
1. More to Come 13
1.1. Send in Your Feedback 14

Chapter 1. Red Hat Network Overview **15**
1.1. Update 16
1.2. Management 16
1.3. Provisioning 17
1.4. Monitoring 17
1.5. Errata Notifications and Scheduled Package Installations 18
1.6. Security, Quality Assurance, and Red Hat Network 18
1.7. Before You Begin 19

Chapter 2. Red Hat Update Agent **21**
2.1. Starting the Red Hat Update Agent 21
2.2. Registration 23
2.2.1. Registering a User Account 24
2.2.2. Activate 26
2.2.3. Channels 28
2.2.4. Packages Flagged to be Skipped 29
2.2.5. Available Package Updates 29
2.2.6. Retrieving Packages 30
2.2.7. Installing Packages 31
2.3. Command Line Version 33
2.3.1. Installing the Red Hat GPG key 35
2.3.2. Manual Package Installation 37
2.3.3. Synchronizing Your System Profile 37
2.3.4. Log File 38
2.4. Configuration 38
2.4.1. Using the Red Hat Update Agent Configuration Tool 38
2.4.1.1. General Settings 38
2.4.1.2. Retrieval/Installation Settings 39
2.4.1.3. Package Exceptions Settings 40
2.4.2. Command Line Version 41
2.5. Registering with Activation Keys 42

Chapter 3. Red Hat Network Daemon **45**
3.1. Configuring 45
3.2. Viewing Status 45
3.3. Disabling 45
3.4. Troubleshooting 45

Chapter 4. Red Hat Network Alert Notification Tool **47**
4.1. Configuring the Applet 47
4.2. Notification Icons 48
4.3. Viewing Updates 49
4.4. Applying Updates 49
4.5. Launching the RHN Website 50

Chapter 5. Red Hat Network Registration Client **51**
5.1. Configuring the Red Hat Network Registration Client 51
5.2. Starting the Red Hat Network Registration Client 52
5.3. Registering a User Account 54

5.4. Registering a System Profile 56
5.4.1. Hardware System Profile 56
5.4.2. Software System Profile 57
5.4.2.1. Gathering RPM Database Information 57
5.4.2.2. Choosing RPM Packages to Exclude from the System Profile 58
5.5. Finishing Registration 59
5.6. Entitling Your System 60
5.7. Text Mode RHN Registration Client 61

Chapter 6. Red Hat Network Website **62**
6.1. Navigation 62
6.1.1. Entitlement Views 62
6.1.2. Categories and Pages 63
6.1.3. Errata Alert Icons 64
6.1.4. Quick Search 65
6.1.5. Systems Selected 65
6.1.6. Lists 65
6.2. Logging into the RHN Website 65
6.3. Your RHN 66
6.3.1. Your Account 68
6.3.1.1. Addresses 68
6.3.1.2. Change Email 68
6.3.1.3. Account Deactivation 68
6.3.2. Your Preferences 68
6.3.3. Locale Preferences 69
6.3.4. Subscription Management 69
6.3.4.1. System Entitlements 70
6.3.4.2. Virtualization Entitlements 70
6.3.4.3. Software Channel Entitlements 71
6.3.4.4. Purchase or Renew 71
6.3.4.5. Expiration Dates &Purchase History 71
6.4. Systems 71
6.4.1. Overview — 71
6.4.2. Systems 72
6.4.2.1. All 73
6.4.2.2. Virtual Systems 73
6.4.2.3. Out of Date 73
6.4.2.4. Unentitled — 73
6.4.2.5. Ungrouped 73
6.4.2.6. Inactive 73
6.4.2.7. Satellite 74
6.4.2.8. Proxy 74
6.4.2.9. System Details 74
6.4.2.9.1. System Details ⇒ Details 75
6.4.2.9.1.1. System Details ⇒ Details ⇒ Overview 75
6.4.2.9.1.2. System Details ⇒ Details ⇒ Properties 78
6.4.2.9.1.3. System Details ⇒ Details ⇒ Remote Command — 79
6.4.2.9.1.4. System Details ⇒ Details ⇒ Reactivation — 79
6.4.2.9.1.5. System Details ⇒ Details ⇒ Hardware 80
6.4.2.9.1.6. System Details ⇒ Details ⇒ Notes 80
6.4.2.9.1.7. System Details ⇒ Details ⇒ Custom Info — 80
6.4.2.9.1.8. System Details ⇒ Details ⇒ Proxy 80
6.4.2.9.1.9. System Details ⇒ Details ⇒ Satellite 80
6.4.2.9.2. System Details ⇒ Software 80
6.4.2.9.2.1. System Details ⇒ Software ⇒ Errata 80
6.4.2.9.2.2. System Details ⇒ Software ⇒ Packages 81

6.4.2.9.2.3. System Details ⇒ Software ⇒ Software Channels 82
6.4.2.9.3. System Details ⇒ Configuration — 82
6.4.2.9.3.1. System Details ⇒ Configuration ⇒ Overview 83
6.4.2.9.3.2. System Details ⇒ Configuration ⇒ Managed Files 83
6.4.2.9.3.3. System Details ⇒ Configuration ⇒ Compare Files 83
6.4.2.9.3.4. System Details ⇒ Configuration ⇒ Manage Configuration Channels 83
6.4.2.9.3.5. System Details ⇒ Configuration ⇒ Local Overrides 84
6.4.2.9.3.6. System Details ⇒ Configuration ⇒ Sandbox 84
6.4.2.9.4. System Details ⇒ Provisioning — 84
6.4.2.9.4.1. System Details ⇒ Provisioning ⇒ Kickstart — 84
6.4.2.9.4.2. System Details ⇒ Provisioning ⇒ Snapshots — 85
6.4.2.9.4.3. System Details ⇒ Provisioning ⇒ Snapshot Tags — 85
6.4.2.9.5. System Details ⇒ Virtualization 85
6.4.2.9.5.1. System Details ⇒ Virtualization ⇒ Details 86
6.4.2.9.5.2. System Details ⇒ Monitoring — 86
6.4.2.9.5.3. System Details ⇒ Groups — 87
6.4.2.9.5.3.1. System Details ⇒ Groups ⇒ List/Leave — 87
6.4.2.9.5.3.2. System Details ⇒ Groups ⇒ Join — 87
6.4.2.9.5.4. System Details ⇒ Events 87
6.4.2.9.5.4.1. System Details ⇒ Events ⇒ Pending 87
6.4.2.9.5.4.2. System Details ⇒ Events ⇒ History 87
6.4.3. System Groups — 87
6.4.3.1. Creating Groups 88
6.4.3.2. Adding and Removing Systems in Groups 88
6.4.3.3. System Group Details — 89
6.4.3.3.1. System Group Details ⇒ Details — 89
6.4.3.3.2. System Group Details ⇒ Systems — 89
6.4.3.3.3. System Group Details ⇒ Target Systems — 89
6.4.3.3.4. System Group Details ⇒ Errata — 89
6.4.3.3.5. System Group Details ⇒ Admins — 89
6.4.4. System Set Manager — 89
6.4.4.1. System Set Manager ⇒ Overview — 90
6.4.4.2. System Set Manager ⇒ Systems — 90
6.4.4.3. System Set Manager ⇒ Errata — 90
6.4.4.4. System Set Manager ⇒ Packages — 90
6.4.4.4.1. System Set Manager ⇒ Packages ⇒ Upgrade — 90
6.4.4.4.2. System Set Manager ⇒ Packages ⇒ Install — 91
6.4.4.4.3. System Set Manager ⇒ Packages ⇒ Remove — 91
6.4.4.5. System Set Manager ⇒ Verify 91
6.4.4.6. System Set Manager ⇒ Patches 91
6.4.4.7. System Set Manager ⇒ Patch Clusters 91
6.4.4.8. System Set Manager ⇒ Groups — 91
6.4.4.9. System Set Manager ⇒ Channels — 91
6.4.4.9.1. System Set Manager ⇒ Channels ⇒ Channel Subscriptions — 91
6.4.4.9.2. System Set Manager ⇒ Channels ⇒ Config Channels — 92
6.4.4.9.2.1. System Set Manager ⇒ Channels ⇒ Config Channels ⇒ Deploy — 92
6.4.4.9.2.2. System Set Manager ⇒ Channels ⇒ Config Channels ⇒ Diff — 92
6.4.4.9.2.3. System Set Manager ⇒ Channels ⇒ Config Channels ⇒ Subscriptions — 92
6.4.4.9.3. System Set Manager ⇒ Channels ⇒ Base Channel Alteration — 93
6.4.4.10. System Set Manager ⇒ Provisioning — 93
6.4.4.10.1. System Set Manager ⇒ Provisioning ⇒ Kickstart — 93
6.4.4.10.2. System Set Manager ⇒ Provisioning ⇒ Tag Systems — 93
6.4.4.10.3. System Set Manager ⇒ Provisioning ⇒ Rollback — 93
6.4.4.10.4. System Set Manager ⇒ Provisioning ⇒ Remote Command — 93
6.4.4.11. System Set Manager ⇒ Misc — 93

6.4.4.11.1. System Set Manager ⇒ Misc ⇒ System Profile Updates — 93
6.4.4.11.2. System Set Manager ⇒ Misc ⇒ Custom System Information — 94
6.4.4.11.3. System Set Manager ⇒ Misc ⇒ Reboot Systems — 94
6.4.4.11.4. System Set Manager ⇒ Misc ⇒ Lock Systems — 94
6.4.4.11.5. System Set Manager ⇒ Misc ⇒ Delete Systems — 94
6.4.4.11.6. System Set Manager ⇒ Misc ⇒ Add or Remove Add-On Entitlements — 94
6.4.4.11.7. System Set Manager ⇒ Misc ⇒ System Preferences — 94
6.4.5. Advanced Search — 95
6.4.6. Activation Keys — 95
6.4.6.1. Managing Activation Keys 95
6.4.6.2. Using Multiple Activation Keys at Once — 96
6.4.7. Stored Profiles — 97
6.4.8. Custom System Info — 97
6.4.9. Kickstart — 97
6.4.9.1. Introduction to Kickstart 98
6.4.9.1.1. Kickstart Explained 98
6.4.9.1.2. Kickstart Prerequisites 99
6.4.9.1.3. Building Bootable Kickstart ISOs 99
6.4.9.1.4. Integrating Kickstart with PXE 100
6.4.9.2. View a List of Kickstart Profiles 100
6.4.9.3. Create a New Kickstart Profile 101
6.4.9.3.1. Kickstart Details ⇒ Details — 101
6.4.9.3.2. Kickstart Details ⇒ Operating System — 102
6.4.9.3.3. Kickstart Details ⇒ Advanced Options — 102
6.4.9.3.4. Kickstart Details ⇒ Bare Metal Kickstart — 102
6.4.9.3.5. System Details ⇒ Details — 102
6.4.9.3.6. System Details ⇒ Locale — 103
6.4.9.3.7. System Details ⇒ Partitioning — 103
6.4.9.3.8. System Details ⇒ File Preservation — 103
6.4.9.3.9. System Details ⇒ GPG and SSL — 103
6.4.9.3.10. System Details ⇒ Troubleshooting — 103
6.4.9.3.11. Software ⇒ Package Groups — 103
6.4.9.3.12. Software ⇒ Package Profiles — 104
6.4.9.3.13. Activation Keys — 104
6.4.9.3.14. Scripts — 104
6.4.9.3.15. Kickstart File — 105
6.4.9.4. Kickstart ⇒ Bare Metal — 105
6.4.9.5. Kickstart ⇒ GPG and SSL Keys — 105
6.4.9.6. Kickstart ⇒ Distributions — 105
6.4.9.7. Kickstart ⇒ File Preservation — 106
6.5. Errata 106
6.5.1. Relevant Errata 107
6.5.2. All Errata 108
6.5.2.1. Apply Errata Updates 108
6.5.2.2. Errata Details 109
6.5.2.2.1. Errata Details ⇒ Details 109
6.5.2.2.2. Errata Details ⇒ Packages 109
6.5.2.2.3. Errata Details ⇒ Affected Systems 110
6.5.3. Advanced Search 110
6.6. Channels 110
6.6.1. Software Channels 110
6.6.1.1. Relevant Channels 111
6.6.1.2. Retired Channels 111
6.6.1.3. All Channels 111
6.6.1.4. Software Channel Details 111

6.6.1.4.1. Software Channel Details ⇒ Details 111
6.6.1.4.2. Software Channel Details ⇒ Subscribers — 112
6.6.1.4.3. Software Channel Details ⇒ Managers — 112
6.6.1.4.4. Software Channel Details ⇒ Errata 112
6.6.1.4.5. Software Channel Details ⇒ Packages 112
6.6.1.4.6. Software Channel Details ⇒ Subscribed Systems 113
6.6.1.4.7. Software Channel Details ⇒ Target Systems 113
6.6.1.4.8. Software Channel Details ⇒ Downloads 113
6.6.1.4.9. Software Channel Details ⇒ License 113
6.6.2. Channel Entitlements 113
6.6.3. Download Software 113
6.6.3.1. Relevant ISOs 114
6.6.3.2. All ISOs 114
6.6.4. Package Search 114
6.6.5. Manage Software Channels 114
6.6.5.1. Manage Software Channels ⇒ Channel Details 114
6.6.5.1.1. Manage Software Channels ⇒ Channel Details ⇒ Channel Details 114
6.6.5.1.2. Manage Software Channels ⇒ Channel Details ⇒ Managers 114
6.6.5.1.3. Manage Software Channels ⇒ Channel Details ⇒ Errata 115
6.6.5.1.4. Manage Software Channels ⇒ Channel Details ⇒ Packages 115
6.6.5.2. Manage Software Channels ⇒ Manage Software Packages 115
6.6.6. Manage Config Channels — 115
6.6.6.1. Preparing Systems for Config Management 116
6.6.6.2. Manage Config Channels ⇒ Config Channels — 116
6.6.6.2.1. Manage Config Channels ⇒ Config Channels ⇒ Global — 116
6.6.6.2.2. Manage Config Channels ⇒ Config Channels ⇒ System — 116
6.6.6.3. Manage Config Channels ⇒ Manage Files — 116
6.6.6.4. Manage Config Channels ⇒ Quota — 117
6.6.6.5. Configuration Channel Details — 117
6.6.6.5.1. Configuration Channel Details ⇒ Details — 117
6.6.6.5.2. Configuration Channel Details ⇒ Files — 117
6.6.6.5.2.1. Configuration Channel Details ⇒ Files ⇒ List — 117
6.6.6.5.2.2. Configuration Channel Details ⇒ Files ⇒ Upload — 117
6.6.6.5.2.3. Configuration Channel Details ⇒ Files ⇒ Create File — 117
6.6.6.5.2.4. Configuration Channel Details ⇒ Files ⇒ Create Directory — 118
6.6.6.5.3. Configuration Channel Details ⇒ Systems — 118
6.6.6.5.4. Configuration Channel Details ⇒ Target Systems — 118
6.6.6.6. Configuration File Details — 118
6.6.6.6.1. Configuration File Details ⇒ Details — 118
6.6.6.6.2. Configuration File Details ⇒ Revisions — 118
6.6.6.6.3. Configuration File Details ⇒ Diff — 119
6.6.6.6.4. Configuration File Details ⇒ Copy — 119
6.6.6.7. Including Macros in your Configuration Files 119
6.7. Schedule 120
6.7.1. Pending Actions 121
6.7.2. Failed Actions 121
6.7.3. Completed Actions 121
6.7.4. Archived Actions 121
6.7.5. Actions List 122
6.7.5.1. Action Details 122
6.7.5.1.1. Action Details ⇒ Details 122
6.7.5.1.2. Action Details ⇒ Completed Systems 122
6.7.5.1.3. Action Details ⇒ In Progress Systems 122
6.7.5.1.4. Action Details ⇒ Failed Systems 122
6.8. Users — 122

6.8.1. User List ⇒ Active — 123
6.8.1.1. User List ⇒ Active ⇒ User Details — 124
6.8.1.1.1. User List ⇒ Active ⇒ User Details ⇒ Details — 125
6.8.1.1.2. User List ⇒ Active ⇒ User Details ⇒ System Groups — 126
6.8.1.1.3. User List ⇒ Active ⇒ User Details ⇒ Systems — 126
6.8.1.1.4. User List ⇒ Active ⇒ User Details ⇒ Channel Permissions — 126
6.8.1.1.4.1. User List ⇒ Active ⇒ User Details ⇒ Channel Permissions ⇒ Subscription —
6.8.1.1.4.2. User List ⇒ Active ⇒ User Details ⇒ Channel Permissions ⇒ 126
Management — 126
6.8.1.1.5. User List ⇒ Active ⇒ User Details ⇒ Preferences — 126
6.8.1.1.6. User List ⇒ Active ⇒ User Details ⇒ Addresses — 127
6.8.1.1.7. User List ⇒ Active ⇒ User Details ⇒ Notification Methods — 127
6.8.2. User List ⇒ Deactivated — 127
6.8.3. User List ⇒ All — 127
6.9. Monitoring — 127
6.9.1. Probe Status — 128
6.9.1.1. Probe Status ⇒ Critical — 128
6.9.1.2. Probe Status ⇒ Warning — 128
6.9.1.3. Probe Status ⇒ Unknown — 129
6.9.1.4. Probe Status ⇒ Pending — 129
6.9.1.5. Probe Status ⇒ OK — 129
6.9.1.6. Probe Status ⇒ All — 129
6.9.1.7. Current State — 129
6.9.2. Notification — 129
6.9.2.1. Notification ⇒ Filters 129
6.9.2.1.1. Notification ⇒ Notification Filters ⇒ Active Filters 130
6.9.2.1.2. Notification ⇒ Notification Filters ⇒ Expired Filters 130
6.9.3. Probe Suites 131
6.9.4. Scout Config Push — 132
6.9.5. General Config — 132
6.10. Satellite Tools 133
6.10.1. Satellite Tools ⇒ Satellite Configuration 133
6.10.1.1. Satellite Tools ⇒ Satellite Configuration ⇒ General 133
6.10.1.2. Satellite Tools ⇒ Satellite Configuration ⇒ Monitoring 133
6.10.1.3. Satellite Tools ⇒ Satellite Configuration ⇒ Certificate 133
6.10.1.4. Satellite Tools ⇒ Satellite Configuration ⇒ Bootstrap 134
6.10.1.5. Satellite Tools ⇒ Satellite Configuration ⇒ Restart 134
6.11. Help 134
6.11.1. Help Desk 134
6.11.2. Quick Start Guide 134
6.11.3. FAQ 134
6.11.4. Migration FAQ 134
6.11.5. Reference Guide 134
6.11.6. Best Practices Guide 135
6.11.7. Contact RHN 135
6.11.8. Satellite Installation Guide 135
6.11.9. Proxy Guide 135
6.11.10. Client Configuration Guide 135
6.11.11. Channel Management Guide 135
6.11.12. Terms &Conditions 135
6.11.13. Outage Policy 135
6.11.14. Release Notes 135
6.11.15. Get RHN Software 135

Chapter 7. Monitoring **137**
7.1. Prerequisites 137

7.2. Red Hat Network Monitoring Daemon (rhnmd) 137
7.2.1. Probes requiring the daemon 137
7.2.2. Installing the Red Hat Network Monitoring Daemon 138
7.2.3. Configuring SSH 139
7.2.4. Installing the SSH key 139
7.3. mysql-server package 140
7.4. Notifications 140
7.4.1. Creating Notification Methods 140
7.4.2. Receiving Notifications 141
7.4.3. Redirecting Notifications 141
7.4.4. Filtering Notifications 142
7.4.5. Deleting Notification Methods 142
7.5. Probes 143
7.5.1. Managing Probes 143
7.5.2. Establishing Thresholds 144
7.5.3. Monitoring the RHN Server 144
7.6. Troubleshooting 144
7.6.1. Examining Probes with rhn-catalog 144
7.6.2. Viewing the output of rhn-runprobe 145

Chapter 8. Virtualization 147
8.1. Setting Up the Host System for Your Virtual Systems 147
8.1.1. Create a Kickstart Profile for the Guest Systems 147
8.1.2. Kickstart Your Host System 148
8.1.2.1. Your Host System Has Red Hat Enterprise Linux 4 or Earlier Installed 148
8.1.2.2. You Host System Does Not have Red Hat Enterprise Linux Installed 149
8.1.2.3. Your Host System Has Red Hat Enterprise Linux 5 Installed 150
8.2. Setting Up Your Virtual Systems 152
8.2.1. Create a Kickstart Profile for the Guest Systems 152
8.2.2. Provision Your Guest Systems 153
8.3. Working With Your Virtual Systems 154
8.3.1. Logging into Virtual Systems Directly via SSH 154
8.3.2. Gaining Console Access Via the Host 154
8.3.3. Installing Software Via the Satellite Web Interface 155
8.3.4. Installing Software Via Yum From the Virtual System 155
8.3.5. Deleting Virtual Systems 155

Chapter 9. UNIX Support Guide 157
9.1. Introduction 157
9.1.1. Supported UNIX Variants 157
9.1.2. Prerequisites 157
9.1.3. Included Features 157
9.1.4. Differences in Functionality 157
9.1.5. Excluded Features 158
9.2. Satellite Server Preparation/Configuration 158
9.3. Client System Preparation 160
9.3.1. Download and Install Additional Packages 160
9.3.1.1. Install Third-Party Packages 160
9.3.1.2. Configure the Library Search Path 161
9.3.1.3. Download RHN Client Packages 161
9.3.1.4. Install the RHN Packages 162
9.3.1.5. Include RHN Packages in the PATH 162
9.3.2. Deploying Client SSL Certificates 163
9.3.3. Configuring the clients 163
9.4. Registration and Updates 164
9.4.1. Registering Systems 164

9.4.2. Obtaining Updates 165
9.4.2.1. Uploading Packages to the Satellite 165
9.4.2.1.1. solaris2mpm 165
9.4.2.1.2. rhnpush with .mpm Files 166
9.4.2.2. Updating Through the Website 167
9.4.2.3. Updating From the Command Line 168
9.5. Remote Commands 168
9.5.1. Enabling Commands 168
9.5.2. Issuing Commands 169

Command Line Config Management Tools 170
A.1. Red Hat Network Actions Control 170
A.1.1. General command line options 170
A.2. Red Hat Network Configuration Client 171
A.2.1. Listing Config Files 171
A.2.2. Getting a Config File 172
A.2.3. Viewing Config Channels 172
A.2.4. Differentiating between Config Files 172
A.2.5. Verifying Config Files 173
A.3. Red Hat Network Configuration Manager 173
A.3.1. Creating a Config Channel 174
A.3.2. Adding Files to a Config Channel 174
A.3.3. Differentiating between Latest Config Files 175
A.3.4. Differentiating between Various Versions 175
A.3.5. Downloading All Files in a Channel 176
A.3.6. Getting the Contents of a File 176
A.3.7. Listing All Files in a Channel 177
A.3.8. Listing All Config Channels 177
A.3.9. Removing a File from a Channel 177
A.3.10. Deleting a Config Channel 178
A.3.11. Determining the Number of File Revisions 178
A.3.12. Updating a File in a Channel 178
A.3.13. Uploading Multiple Files at Once 179

RHN API Access 180
B.1. Using the auth Class and Getting the Session 180
B.2. Obtaining the system_id 180
B.3. Determining the sid 180
B.4. Viewing the cid 180
B.5. Getting the sgid 180
B.6. Channel Labels 181
B.7. Sample API Script 181

Probes 183
C.1. Probe Guidelines 183
C.2. Apache 1.3.x and 2.0.x 184
C.2.1. Apache::Processes 184
C.2.2. Apache::Traffic 185
C.2.3. Apache::Uptime 185
C.3. BEA WebLogic 6.x and higher 186
C.3.1. BEA WebLogic::Execute Queue 186
C.3.2. BEA WebLogic::Heap Free 187
C.3.3. BEA WebLogic::JDBC Connection Pool 187
C.3.4. BEA WebLogic::Server State 188
C.3.5. BEA WebLogic::Servlet 188
C.4. General 189

C.4.1. General::Remote Program 189
C.4.2. General::Remote Program with Data 189
C.4.3. General::SNMP Check 190
C.4.4. General::TCP Check 191
C.4.5. General::UDP Check 191
C.4.6. General::Uptime (SNMP) 192
C.5. Linux 192
C.5.1. Linux::CPU Usage 192
C.5.2. Linux::Disk IO Throughput 193
C.5.3. Linux::Disk Usage 193
C.5.4. Linux::Inodes 194
C.5.5. Linux::Interface Traffic 194
C.5.6. Linux::Load 195
C.5.7. Linux::Memory Usage 195
C.5.8. Linux::Process Counts by State 196
C.5.9. Linux::Process Count Total 196
C.5.10. Linux::Process Health 197
C.5.11. Linux::Process Running 198
C.5.12. Linux::Swap Usage 199
C.5.13. Linux::TCP Connections by State 199
C.5.14. Linux::Users 200
C.5.15. Linux::Virtual Memory 200
C.6. LogAgent 201
C.6.1. LogAgent::Log Pattern Match 201
C.6.2. LogAgent::Log Size 202
C.7. MySQL 3.23 - 3.33 203
C.7.1. MySQL::Database Accessibility 203
C.7.2. MySQL::Opened Tables 204
C.7.3. MySQL::Open Tables 204
C.7.4. MySQL::Query Rate 204
C.7.5. MySQL::Threads Running 205
C.8. Network Services 205
C.8.1. Network Services::DNS Lookup 205
C.8.2. Network Services::FTP 206
C.8.3. Network Services::IMAP Mail 206
C.8.4. Network Services::Mail Transfer (SMTP) 207
C.8.5. Network Services::Ping 207
C.8.6. Network Services::POP Mail 208
C.8.7. Network Services::Remote Ping 208
C.8.8. Network Services::RPCService 209
C.8.9. Network Services::Secure Web Server (HTTPS) 209
C.8.10. Network Services::SSH 210
C.8.11. Network Services::Web Server (HTTP) 210
C.9. Oracle 8i and 9i 211
C.9.1. Oracle::Active Sessions 212
C.9.2. Oracle::Availability 212
C.9.3. Oracle::Blocking Sessions 212
C.9.4. Oracle::Buffer Cache 213
C.9.5. Oracle::Client Connectivity 213
C.9.6. Oracle::Data Dictionary Cache 214
C.9.7. Oracle::Disk Sort Ratio 214
C.9.8. Oracle::Idle Sessions 215
C.9.9. Oracle::Index Extents 215
C.9.10. Oracle::Library Cache 216
C.9.11. Oracle::Locks 216

C.9.12. Oracle::Redo Log 217
C.9.13. Oracle::Table Extents 217
C.9.14. Oracle::Tablespace Usage 218
C.9.15. Oracle::TNS Ping 219
C.10. RHN Satellite 219
C.10.1. RHN Satellite::Disk Space 219
C.10.2. RHN Satellite::Execution Time 220
C.10.3. RHN Satellite::Interface Traffic 220
C.10.4. RHN Satellite::Latency 220
C.10.5. RHN Satellite::Load 221
C.10.6. RHN Satellite::Probe Count 221
C.10.7. RHN Satellite::Process Counts 221
C.10.8. RHN Satellite::Processes 222
C.10.9. RHN Satellite::Process Health 222
C.10.10. RHN Satellite::Process Running 223
C.10.11. RHN Satellite::Swap 223
C.10.12. RHN Satellite::Users 224

Glossary **224**
A 224
B 224
C 224
D 225
E 225
M 226
N 226
O 226
P 226
R 227
S 228
U 228
V 229
Y 229

Index **229**
A 229
B 230
C 230
D 231
E 232
G 232
H 233
I 233
K 233
L 233
M 234
N 235
O 235
P 236
Q 239
R 239
S 242
T 245
U 245
V 245
W 246

Y 246

Introduction to the Guide

Welcome to the *Red Hat Network 5.0.0 Reference Guide*. The *RHN Reference Guide* guides you through registering systems with Red Hat Network and using its many features.

Since Red Hat Network offers a variety of service levels, from the most basic Update module to the most advanced Monitoring package, some content of this guide may be inapplicable to you. This is particularly true of the RHN website, which displays selected categories, pages, and tabs depending on the entitlement level of the account used to log in. Refer to Chapter 6, *Red Hat Network Website* to determine what is available to you.

Depending on the version of Red Hat Enterprise Linux installed and the addition of new features, the **Red Hat Network Registration Client** and the **Red Hat Update Agent** may differ from the descriptions in this manual. Use Red Hat Network to update these applications before referring to the latest version of this manual.

All versions of this manual are available in HTML and PDF formats at http://www.redhat.com/docs/manuals/RHNetwork/.

This version of the manual covers version 4.4.5 of the Red Hat Enterprise Linux 3 and 4 **Red Hat Update Agent** and versions 2.9.14 and 2.9.12 of the Red Hat Enterprise Linux 2.1 **Red Hat Update Agent** and **Red Hat Network Registration Client**, respectively.

Warning

Systems running Red Hat Enterprise Linux 2.1 must use the **Red Hat Network Registration Client** before starting the **Red Hat Update Agent**. Refer to Chapter 5, ***Red Hat Network Registration Client*** for instructions. Systems running Red Hat Enterprise Linux 3, Red Hat Enterprise Linux 4 and later register with the **Red Hat Update Agent**. Refer to Chapter 2, ***Red Hat Update Agent*** for instructions.

For an overview of Red Hat Network offerings, please review the descriptions available at http://www.redhat.com/software/rhn/.

1. More to Come

The *Red Hat Network Reference Guide* is constantly expanding as new Red Hat Network features and service plans are launched. HTML and PDF versions of this and other manuals are available within the **`Help`** section of the RHN website and at http://www.redhat.com/docs/.

Note

Although this manual reflects the most current information possible, read the *RHN Release Notes* for information that may not have been available prior to the finalization of the documentation. The notes can be found on the RHN website and at http://www.redhat.com/docs/manuals/RHNetwork/.

The following RHN documentation has been translated for the RHN 4.0 release: RHN 3.7 Reference Guide, RHN 3.7 Satellite Guide, RHN 3.7 Release Notes, and the RHN 4.0 Release Notes. Translations of the remaining RHN 4.0 documentation will be available after the initial release. Translated documentation is available at http://rhn.redhat.com/help/

1.1. Send in Your Feedback

If you would like to make suggestions about the *Red Hat Network Reference Guide*, please submit a report in Bugzilla: http://bugzilla.redhat.com/bugzilla/

Be sure to select the Red Hat Network product and the Documentation component. To easily associate the problem with this guide, mention its identifier:

Red Hat Network Reference Guide"

Chapter 1. Red Hat Network Overview

Have you ever read about a new version of a software package and wanted to install it but could not find it?

Have you ever tried to find an RPM through an Internet search engine or an RPM repository and been linked to an unknown site?

Have you ever tried to find an RPM but instead found only source files that you had to compile yourself?

Have you ever spent hours or even days visiting different websites to see if you have the latest packages installed on your system, only to have to do it again in a few months?

Those days are over with Red Hat Network (RHN). RHN provides the solution to all your system software management needs.

Red Hat Network is an Internet solution for managing a single Red Hat Enterprise Linux system or a network of Red Hat Enterprise Linux systems. All Security Alerts, Bug Fix Alerts, and Enhancement Alerts (collectively known as Errata Alerts) can be downloaded directly from Red Hat or your own custom collection. You can even schedule updates for delivery to your system immediately after release.

The main components of Red Hat Network are as follows:

- the **Red Hat Update Agent**
- the Red Hat Network website, whether this is hosted by the central RHN Servers, an RHN Satellite, or fed through an RHN Proxy Server
- Red Hat Network Daemon
- the **Red Hat Network Registration Client** - for systems running Red Hat Enterprise Linux 2.1 only.

The **Red Hat Update Agent** (**up2date**) provides your initial connection to Red Hat Network. Red Hat Enterprise Linux 3 and newer systems use the Red Hat Update Agent to register with RHN. Registration involves creating a unique RHN username and password, probing the hardware on your system to create a Hardware Profile, and probing the software packages installed on your system to create a Package Profile. This information is sent to RHN and RHN returns a unique System ID to your system. Once registered, the Red Hat Update Agent enables channel subscription, package installs, and management of System Profiles. See Chapter 2, ***Red Hat Update Agent*** for further information.

The Red Hat Update Agent, as the base component of RHN, is designed to manage a single system. It allows the system's superuser to view and apply Errata to the system. The RHN web interface facilitates the management, monitoring, and provisioning of a large deployment of systems, including the configuration of the Red Hat Update Agent for each system.

The **Red Hat Network Daemon** (**rhnsd**) runs in the background as a service and probes the Red Hat Network for notifications and updates at set time intervals (see Chapter 3, *Red Hat Network Daemon* for further information). This daemon is necessary in order to schedule updates or other actions through the website.

The **Red Hat Network Registration Client** allows you to register your Red Hat Enterprise Linux 2.1 systems with RHN. (Newer versions of Red Hat Enterprise Linux have registration functionality built into the **Red Hat Update Agent**.) See Chapter 5, ***Red Hat Network Registration Client*** for more information.

Many Red Hat Network terms are used throughout this manual. As you read the *Red Hat Network*

Reference Guide, refer to the Glossary as necessary for an explanation of common terms.

Tip

For a comparison chart of RHN service levels, refer to http://www.redhat.com/software/rhn/table/.

1.1. Update

The RHN Update service is ideal for a user with one Red Hat Enterprise Linux system or a small number of Red Hat Enterprise Linux systems. Updated Subscription to Update can be purchased at https://www.redhat.com/apps/commerce/rhn/.

With each Update subscription, you receive the following services:

- Download Software — For customers who have purchased subscriptions to Red Hat Network, ISO images are available for immediate download.
- Priority Access during periods of high load — When Red Hat releases a large erratum, users with Priority Access can be guaranteed that they will be able to access the updated packages immediately.
- RHN Support Access — All paying customers of Red Hat Network receive web based support for their RHN questions.
- Errata Notification, Multiple Systems — Subscriptions for multiple systems means Errata notification for Errata to all of those systems. Note that only one email is distributed per each Erratum, regardless of the number of systems affected.
- Errata Updates, Multiple Systems — Get quick updates for multiple systems with an easy button click for each system.

1.2. Management

In addition to the features offered in the RHN Update subscription level, the RHN Management subscription service allows you to manage your network of Red Hat Enterprise Linux systems, users, and system groups through its **`System Set Manager`** interface.

RHN Management is based upon the concept of an organization. Each Management-level Red Hat customer has the ability to establish users who have administration privileges to system groups. An Organization Administrator has overall control over each Red Hat Network organization with the ability to add and remove systems and users. When users other than the Organization Administrator log into the Red Hat Network website, they see only the systems they have permission to administer.

To create an account that can be used to entitle systems to RHN Management, go to https://rhn.redhat.com/ and click on the **`Create Login`** link under the **`Sign In`** fields. On the *Create a Red Hat Login* page, click **`Create a new Business Login`**. After creating a business account, you may add users within your organization to it.

The Red Hat Network features available to you depend on the subscription level for each Red Hat Enterprise Linux system. With each Management subscription, you receive the functionality provided to Update users, plus:

- Package Profile Comparison — Compare the package set on a system with the package sets of similar systems with one click.

- Search Systems — Search through systems based on a number of criteria: packages, networking information, even hardware asset tags.
- System Grouping — Web servers, database servers, workstations and other workload-focused systems may be grouped so that each set can be administered in common ways.
- Multiple Administrators — Administrators may be given rights to particular system groups, easing the burden of system management over very large organizations.
- System Set Manager — You may now apply actions to sets of systems instead of single systems, work with members of a predefined system group, or work with an ad-hoc collection of systems. Install a single software package to each, subscribe the systems to a new channel, or apply all Errata to them with a single action.
- Batch Processing — Compiling a list of outdated packages for a thousand systems would take days for a dedicated sysadmin. Red Hat Network Management service can do it for you in seconds.

1.3. Provisioning

As the highest management service level, RHN Provisioning encompasses all of the features offered in the RHN Update and Management subscription levels. It is designed to allow you to deploy and manage your network of Red Hat Enterprise Linux systems, users, and system groups.

Like Management, Provisioning is based upon an organization. It takes this concept a step further by enabling customers with Provisioning entitlements to kickstart, reconfigure, track, and revert systems on the fly.

In addition to all of the features mentioned in lower service levels, Provisioning provides:

- Kickstarting — Systems with Provisioning entitlements may be re-installed through RHN with a whole host of options established in kickstart profiles. Options include everything from the type of bootloader and time zone to packages included/excluded and IP address ranges allowed. Even GPG and SSL keys can be pre-configured.
- Client Configuration — RHN Satellite Customers may use RHN to manage the configuration files on Provisioning-entitled systems. Users can upload files to custom configurations channels on the Satellite, verify local configuration files against those stored on the Satellite, and deploy files from the Satellite.
- Snapshot Rollbacks — Provisioning-level users have the ability to revert the package profile and RHN settings of systems. RHN Satellite customers can also roll back local configurations files. This is possible because snapshots are captured whenever an action takes place on a system. These snapshots identify groups, channels, packages, and configuration files.
- Custom System Information — Provisioning customers may identify any type of information they choose about their registered systems. This differs from System Profile information, which is generated automatically, and the Notes, which are unrestricted, in that the Custom System Information allows you to develop specific keys of your choosing and assign searchable values for that key to each Provisioning-entitled system. For instance, this feature allows you to identify the cubicle in which each system is located and search through all registered systems according to their cubicle.

1.4. Monitoring

Monitoring entitlements are available to RHN Satellite customers with Red Hat Enterprise Linux systems.

Monitoring allows an organization to install probes that can immediately detect failures and identify performance degradation before it becomes critical. Used properly, the Monitoring entitlement can

provide insight into the applications, services, and devices on each system.

Specifically, Monitoring provides:

- Probes — Dozens of probes can be run against each system. These range from simple **`ping`** checks to custom remote programs designed to return valuable data.
- Notification — Alerts can be sent to email and pager addresses with contact methods identified by you when a probe changes state. Each probe notification can be sent to a different method, or address.
- Central Status — The results of all probes are summarized in a single **`Probe Status`** page, with the systems affected broken down by state.
- Reporting — By selecting a probe and identifying the particular metric and a range of time, you can generate graphs and event logs depicting precisely how the probe has performed. This can be instrumental in predicting and preventing costly system failures.
- Probe Suites — Groups of probes may be assigned to a system or set of systems at once rather than individually. This allows Administrators to be certain that similar systems are monitored in the same way and saves time configuring individual probes.
- Notification Filters — Probe notifications may be redirected to another recipient, halted, or sent to an additional recipient for a specified time based on probe criteria, notification method, scout or organization.

1.5. Errata Notifications and Scheduled Package Installations

You can configure Red Hat Network to send you email notifications of new and updated software packages as soon as the packages are available through RHN. You receive one email per Erratum, regardless of the number of affected systems. You can also schedule package installs or package updates. The benefits include:

- Reduced time and effort required by system administrators to stay on top of the Red Hat Errata list
- Minimized security vulnerabilities in your network through the application of updates as soon as Red Hat releases them
- Filtered list of package updates (packages not relevant to your network are not included)
- Reliable method of managing multiple systems with similar configurations

1.6. Security, Quality Assurance, and Red Hat Network

Red Hat Network provides significant benefits to your network, including security and quality assurance. All transactions made between your systems and Red Hat Network are encrypted and all RPM packages are signed with Red Hat's GNU Privacy Guard (GPG) signature to ensure authenticity.

Red Hat Network incorporates the following security measures:

1. Your System Profile, available at http://rhn.redhat.com, is accessible only with an RHN-verified username and password.
2. A Digital Certificate is written to the client system after registration and is used to authenticate the system during each transaction between the client and Red Hat Network. The file is only readable by the root user on the client system.
3. Red Hat signs all communications with an electronic signature using GPG. RPM can be used to verify the authenticity of the package before it is installed.
4. Red Hat encrypts all transactions using a Secure Sockets Layer (SSL) connection.

5. The Red Hat Quality Assurance Team tests and verifies all packages before they are added to the Red Hat Errata list and Red Hat Network.

1.7. Before You Begin

By default, all software packages necessary to access Red Hat Network are installed with Red Hat Enterprise Linux distributions. However, if you chose not to install them during the installation process, you must obtain the **Red Hat Update Agent** (**up2date**) and possibly the **Red Hat Network Registration Client** (**rhn_register**). In Red Hat Enterprise Linux 3 and later, registration functionality is built into the **Red Hat Update Agent**, while Red Hat Enterprise Linux 2.1 users will need the **Red Hat Network Registration Client**.

Warning

The SSL certificate packaged with older versions of the **Red Hat Update Agent** and the **Red Hat Network Registration Client** reached its end of life August 28, 2003. Users attempting to connect using this certificate will receive SSL connection or certificate verification errors. You may view and obtain the versions of these applications containing new certificates at the RHN Client Software page. In the RHN website, click **Help** at the top-right corner, **Get RHN Software** in the left navigation bar, and scroll down to examine the packages and versions.

To determine the versions of the client applications installed, run the **rpm -q** command followed by the package name. For instance, for the **Red Hat Network Registration Client**, type the following command:

```
rpm -q rhn_register
```

If the **Red Hat Network Registration Client** is installed, it will return something similar to:

```
rhn_register-2.9.3-1
```

The version number might differ slightly.

If you do not have the **Red Hat Network Registration Client** installed, the command will return:

```
package rhn_register is not installed
```

Perform this check for every package in Table 1.1, “Red Hat Network Packages” that is relevant to your system. Remember, only Red Hat Enterprise Linux 2.1 users need **Red Hat Network Registration Client**. If you prefer to use the command line versions, the two packages ending in **gnome** are not required..

Table 1.1. Red Hat Network Packages

Package Name	Description
rhn_register	Provides the **Red Hat Network Registration Client** program and the text mode interface
rhn_register-gnome	Provides the GNOME interface (graphical version) for the **Red Hat Network Registration Client**; runs if the X Window System is available
up2date	Provides the **Red Hat Update Agent** command line version and the Red Hat Network Daemon
up2date-gnome	Provides the GNOME interface (graphical version) for the **Red Hat Update Agent**; runs if the X Window System is available

Chapter 2. Red Hat Update Agent

The **Red Hat Update Agent** is your connection to Red Hat Network. It enables you to register your systems, create System Profiles, and alter the settings by which your organization and RHN interact. Once registered, your systems can use the **Red Hat Update Agent** to retrieve the latest software packages from Red Hat. This tool allows you to always have the most up-to-date Red Hat Enterprise Linux systems with all security updates, bug fixes, and software package enhancements.

Remember, this tool must be run on the system you wish to update. You cannot use the **Red Hat Update Agent** on the system if it is not entitled to an RHN service offering.

Warning

Only systems running Red Hat Enterprise Linux 3 and later can use the **Red Hat Update Agent** to register with RHN. Systems running Red Hat Enterprise Linux 2.1 must use **Red Hat Network Registration Client** before starting the **Red Hat Update Agent**. Refer to Chapter 5, *Red Hat Network Registration Client* for instructions, then return to this chapter for **Red Hat Update Agent** instructions.

Important

You must use **Red Hat Update Agent** Version 2.5.4 or higher to upgrade your kernel automatically. It installs the updated kernel and configures LILO or GRUB to boot the new kernel the next time the system is rebooted. To ensure that you are running the latest version, execute the command **`up2date up2date`**. If you do not have the latest version installed, this command updates it.

2.1. Starting the Red Hat Update Agent

If you are not running the X Window System or prefer the command line version of the **Red Hat Update Agent**, skip to Section 2.3, “Command Line Version”.

You must be root to run the **Red Hat Update Agent**. If started as a standard user, Red Hat Update Agent prompts you to enter the root password before proceeding. The **Red Hat Update Agent** can be started using one of the following methods:

For Red Hat Enterprise Linux 3 and 4:

- On the GNOME and KDE desktops, go to Applications (the main menu on the panel) => **System Tools** => **Red Hat Network**.
- At a shell prompt (for example, an **xterm** or **gnome-terminal**), type the command **`up2date`**.

For Red Hat Enterprise Linux 2.1:

- On the GNOME desktop, go to the **Main Menu Button** (on the Panel) => **Programs** => **System** => **Update Agent**.
- On the KDE desktop, go to the **Main Menu Button** (on the Panel) => **Update Agent**.
- At a shell prompt (for example, an **xterm** or **gnome-terminal**), type the command **`up2date`**.

If you choose the last option and start the application from a shell prompt, you can specify the options in Table 2.1, "Graphical Update Agent Options". To view these options, type the command **up2date --help**.

For example, use the following command to specify the directory in which to download the updated packages (temporarily overriding your saved configuration):

```
up2date --tmpdir=/tmp/up2date/
```

Table 2.1. Graphical Update Agent Options

Option	Description
--configure	Configure **Red Hat Update Agent** options. Refer to Section 2.4, "Configuration" for detailed instructions.
-d, **--download**	Download packages only; do not install them. This argument temporarily overrides the configuration option **Do not install packages after retrieval.** Use this option if you prefer to install the packages manually.
-f, **--force**	Force package installation. This option temporarily overrides the file, package, and configuration skip lists.
-i, **--install**	Install packages after they are downloaded. This argument temporarily overrides the configuration option **Do not install packages after retrieval.**
-k, **--packagedir**	Specify a colon separated path of directories in which to look for packages before trying to download them.
--nosig	Do not use GPG to check package signatures. This option temporarily overrides the saved configuration option.
--tmpdir=*directory*	Temporarily override the configured package directory. The default location is **/var/spool/up2date**. This option is useful if you do not have enough space in the configured location.
--dbpath=*dir*	Specify an alternate RPM database to use temporarily.

The first time you run the **Red Hat Update Agent**, two dialog boxes appear that you will not see in subsequent startups: **Configure Proxy Server** and **Install GPG Key**.

As shown in Figure 2.1, "Configure Proxy Server", the first dialog box to appear prompts you for HTTP Proxy Server information. This is useful if your network connection requires you to use a proxy server to make HTTP connections. To use this feature, select the **Enable HTTP Proxy** checkbox and type your proxy server in the text field with the format HOST:PORT, such as **squid.mysite.org:3128**. Additionally, if your proxy server requires a username and password, select the **Use Authentication** checkbox and enter your username and password in the respective text fields.

An HTTP Proxy Server is not required by Red Hat Network. If you do not want to use this feature, click the **OK** button without making any selections. Note that the Red Hat Network Server dropdown menu at the top of the dialog box is only useful to RHN Proxy and Satellite customers. These customers should refer to the *RHN Client Configuration Guide* for registration steps. Also note that this dialog box is actually the **General** tab of the **Red Hat Update Agent Configuration Tool**. Refer to Section 2.4, "Configuration" for detailed instructions.

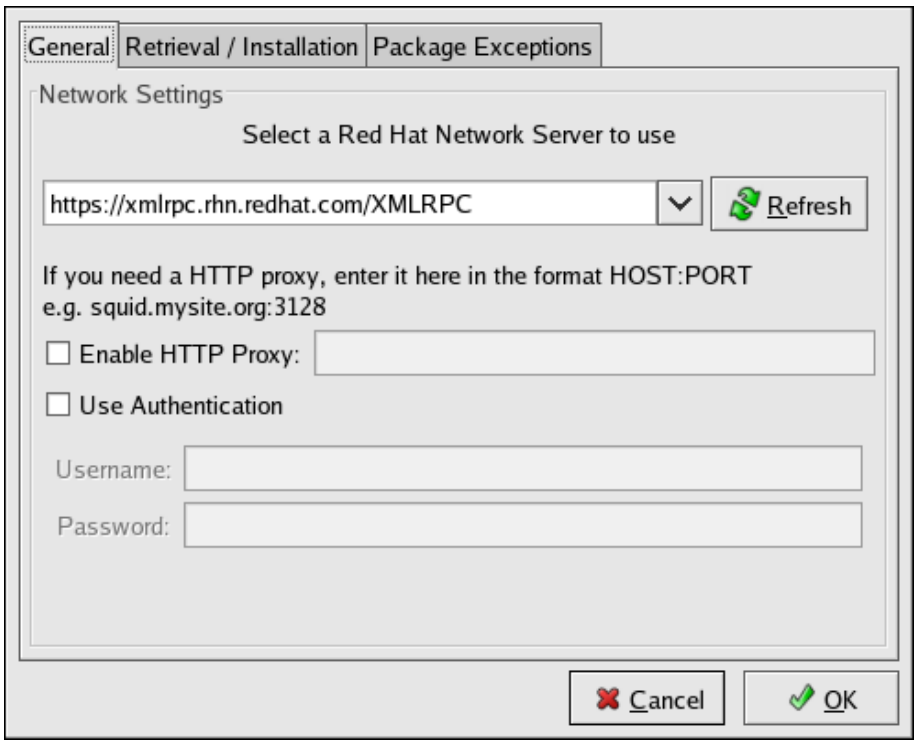


Figure 2.1. Configure Proxy Server

The second dialog box to appear prompts you to install the Red Hat GPG key, as shown in Figure 2.2, "Install GPG Key". This key is used to verify the packages you download for security purposes. Click **Yes** to install the key, and you will not see this message again.

Your GPG keyring does not contain the Red Hat, Inc. public key.
Without it, you will be unable to verify that packages Update Agent downloads are securely signed by Red Hat.
Your Update Agent options specify that you want to use GPG.
Install key?
No
Yes

Figure 2.2. Install GPG Key

2.2. Registration

Before you begin using Red Hat Network, you must create a username, password, and System Profile. Upon launch, the Red Hat Update Agent senses whether these tasks have been accomplished. If not, it guides you through the registration process.

If you ever need to force the Red Hat Update Agent into registration mode, such as to re-register an existing system, you may do so by issuing the following command at a shell prompt:

```
up2date --register
```

Important

If your username is part of a larger organizational account, you should take caution when registering systems. By default, all systems registered with the **Red Hat Update Agent** end up in the Ungrouped section of systems visible only to Organization Administrators. To ensure you retain management of these systems, Red Hat recommends that your organization create an activation key associated with a specific system group and grant you permissions to that group. You may then register your systems using that activation key and find those System Profiles within RHN immediately. Refer to Section 2.5, “Registering with Activation Keys” for instructions.

After installing the Red Hat GPG Key, the screen shown in Figure 2.3, “Welcome Screen” appears. It appears each time you start the Red Hat Update Agent. Click **Forward** to continue.

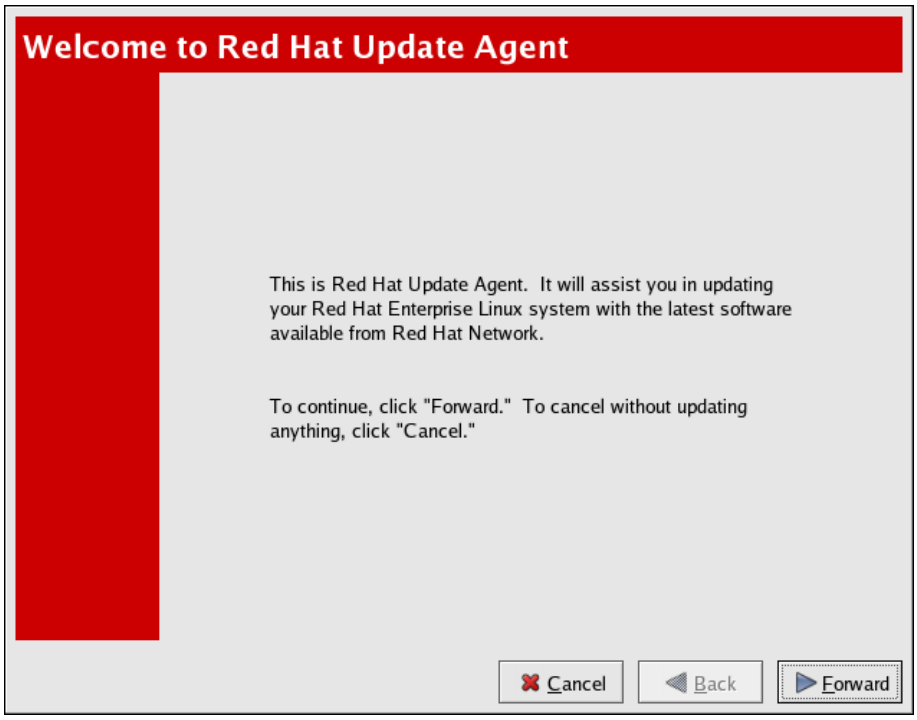

Welcome to Red Hat Update Agent
This is Red Hat Update Agent. It will assist you in updating your Red Hat Enterprise Linux system with the latest software available from Red Hat Network.
To continue, click "Forward." To cancel without updating anything, click "Cancel."
Cancel
Back
Forward

Figure 2.3. Welcome Screen

2.2.1. Registering a User Account

Before you create a System Profile, you must create a user account. Red Hat recommends that you do so through the website at https://rhn.redhat.com/newlogin/, but you may also do so via Red Hat Update Agent (**up2date**).

Important

Users may access and read Red Hat's privacy statement from this screen. Click the **Read our Privacy Statement** button to do so. Red Hat is committed to protecting your privacy. The information gathered during the registration process is used to create a System Profile, which is essential to receiving update notifications about your system. When finished, click **OK**

Those users that have created a Red Hat login previously may enter their username and password and click the **Forward** button to continue.

Users that have registered at least one system with Red Hat Network can add new machines to the same account. To do so, run the Red Hat Update Agent on the new machine and enter the existing Red Hat username and password at this screen.

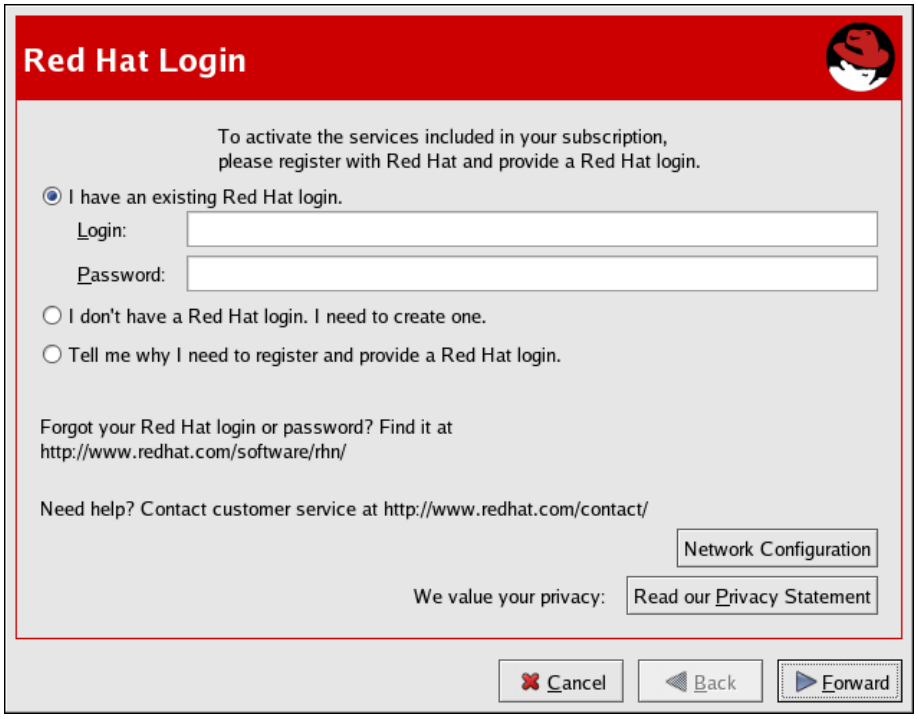

Red Hat Login
To activate the services included in your subscription,
please register with Red Hat and provide a Red Hat login.
I have an existing Red Hat login.
Login:
Password:
I don't have a Red Hat login. I need to create one.
Tell me why I need to register and provide a Red Hat login.
Forgot your Red Hat login or password? Find it at
http://www.redhat.com/software/rhn/
Need help? Contact customer service at http://www.redhat.com/contact/
Network Configuration
We value your privacy:
Read our Privacy Statement
Cancel
Back
Forward

Figure 2.4. Red Hat Login Screen

New users must select the **I don't have a Red Hat login. I need to create one.** radio button and click the **Forward** button. Add details about yourself and your business to the screen shown in Figure 2.5, “Create a User Account”, and identify the methods by which you may be reached.

Your username has the following restrictions:

- Cannot contain any spaces
- Cannot contain the characters & +, %, or '
- Is not case-sensitive, thereby eliminating the possibility of duplicate usernames differing only by capitalization

In addition, the following restrictions apply to both your username and password:

- Must be at least four characters long
- Cannot contain any tabs
- Cannot contain any line feeds

Passwords are case-sensitive for obvious reasons.

Note

You must choose a unique username. If you enter one already in use, you will see an error message. Try different usernames until you find one that has not been used.

Complete all fields marked by an asterisk (*). The address and email addresses are required so that Red Hat may communicate with you regarding your account. You may select to receive monthly copies of Red Hat Magazine, a valuable source of tips, insights, and Red Hat news.

When finished, click **Forward**.

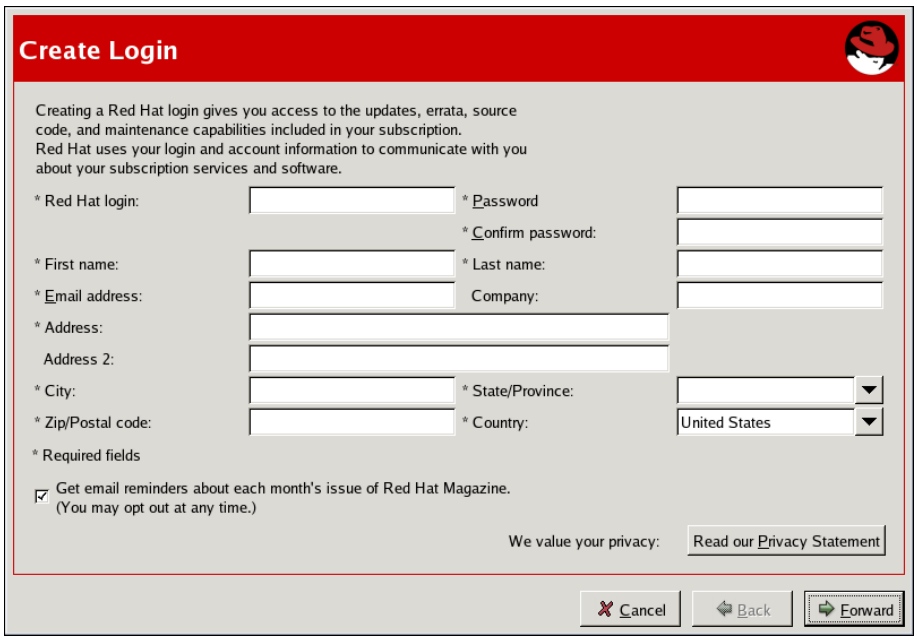

Create Login
Creating a Red Hat login gives you access to the updates, errata, source code, and maintenance capabilities included in your subscription.
Red Hat uses your login and account information to communicate with you about your subscription services and software.
* Red Hat login:
* Password
* Confirm password:
* First name:
* Last name:
* Email address:
Company:
* Address:
Address 2:
* City:
* State/Province:
* Zip/Postal code:
* Country:
United States
* Required fields
Get email reminders about each month's issue of Red Hat Magazine. (You may opt out at any time.)
We value your privacy:
Read our Privacy Statement
Cancel
Back
Forward

Figure 2.5. Create a User Account

2.2.2. Activate

The Activation screen allows you to select various details of your registration. If you have a subscription number, enter it in the appropriate field. If not, select the **Use one of my existing, active subscriptions** radio button.

In the **Connect Your System** option group, select whether to send a hardware or software profile.

After creating a username and password for your Red Hat Network account, the **Red Hat Update Agent** probes your system for the following information:

- Red Hat Enterprise Linux version
- Hostname
- IP address
- CPU model
- CPU speed
- Amount of RAM
- PCI devices

- Disk sizes
- Mount points

The software System Profile consists of a list of RPM packages for which you wish to receive notifications. The **Red Hat Update Agent** displays a list of all RPM packages listed in the RPM database on your system and then allows you to customize the list by deselecting packages.

To see the details of the information gathered from your system, click the **Details** button next to the profile. When finished, click **OK**. If you uncheck the box to the left of the profile, that information is not sent to RHN.

Note

If you do not send a Software Profile, this system will receive no Errata Updates.

Click **Forward** to send the information to RHN.

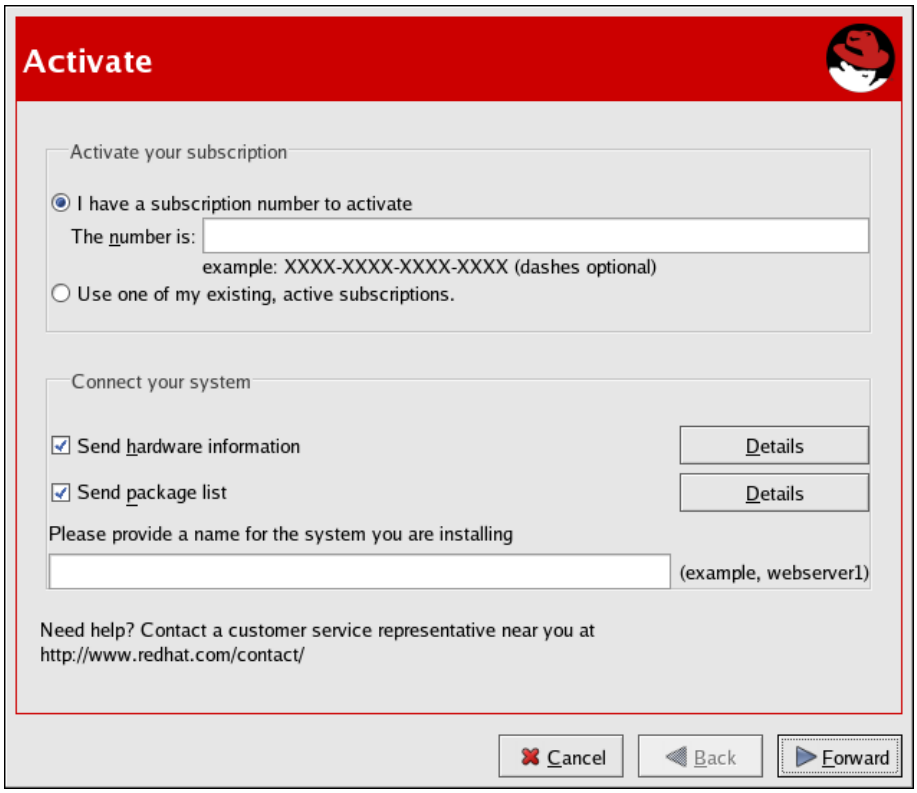


Figure 2.6. Activate

Figure 2.7, “Sending System Profile to Red Hat Network” shows the progress bar displayed as the System Profile is sent.

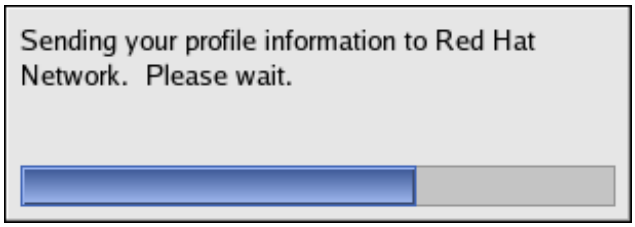


Figure 2.7. Sending System Profile to Red Hat Network

2.2.3. Channels

Red Hat Update Agent next displays all package channels to which you have access. The channels you select from this screen must match the base operating system of the system you are registering. if any child channels are available, such as the **RHEL AS (v.4 for x86) Extras** channel in the figure, you may select them as well. Additional information regarding the selected channel is displayed in the **Channel Information** pane. When finished, click **Forward** to continue.

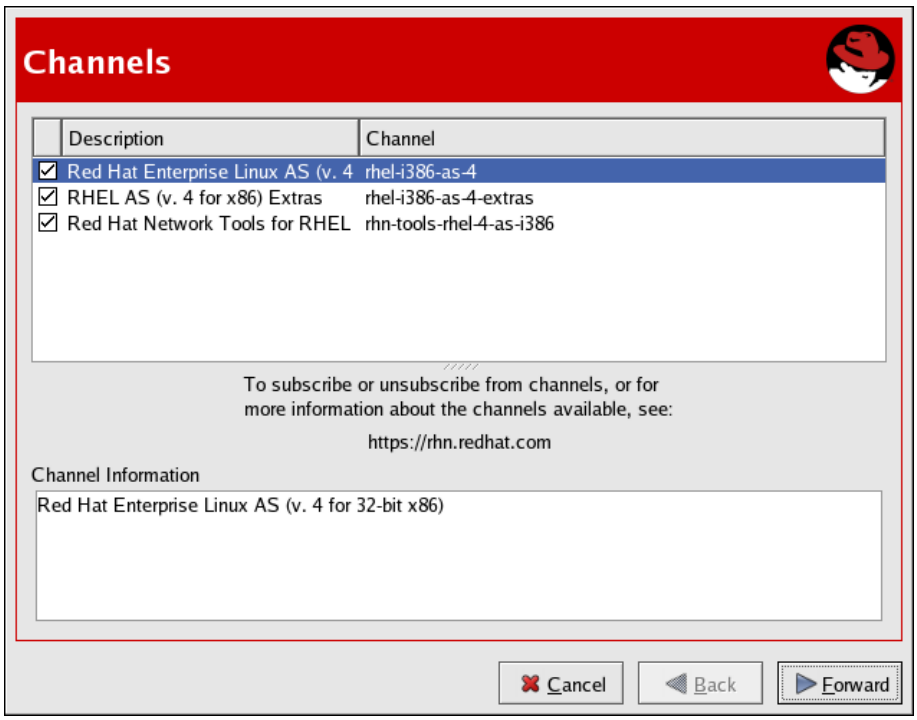


Figure 2.8. Channels

Red Hat Update Agent now compares the packages in your RPM database with those available from the Channel you selected. The progress bar shown in Figure 2.9, “Fetching package list” is displayed during this process.

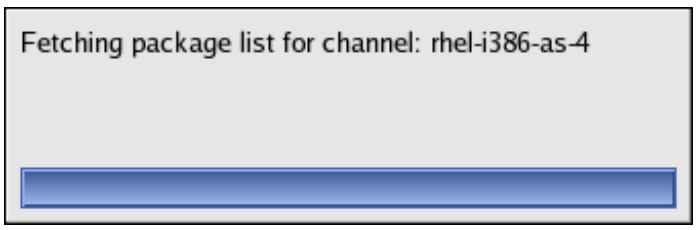


Figure 2.9. Fetching package list

Note

If the version of **up2date** on your system is older than the one in your selected channel, the Red Hat Update Agent asks whether you would like to update it. If you agree, the only package that will be updated is the **up2date** package. This is equivalent to executing the **up2date up2date** command from a shell prompt. Once the updated process has completed, the Red Hat Update Agent restarts and completes the initial update of the system.

2.2.4. Packages Flagged to be Skipped

The next step in the initial update is the selection of files to be skipped. Any packages checked here will not be downloaded and updated by the Red Hat Update Agent. This screen is displayed whenever packages are available that are currently selected to be ignored. You may change these settings at any time from the Red Hat Network Alert Notification Tool. Refer to Chapter 4, *Red Hat Network Alert Notification Tool* for addition information.

Make your selections and click **Forward** to continue.

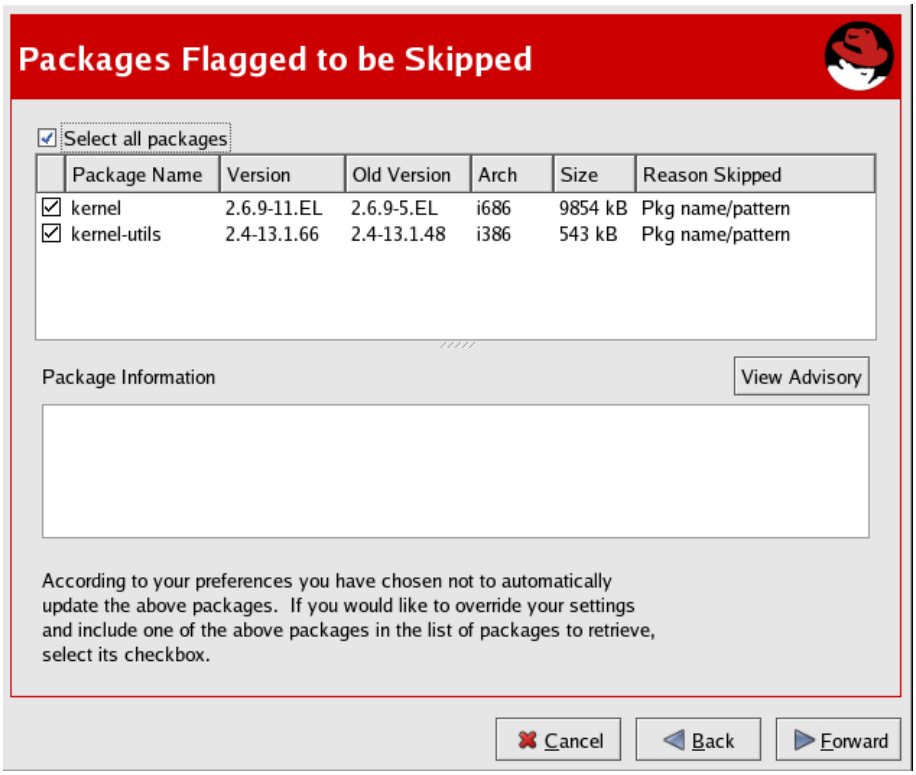


Figure 2.10. Packages Flagged to be Skipped

2.2.5. Available Package Updates

The Red Hat Update Agent next displays all available updates except those you chose to skip in the previous screen. Select those you wish to download and click **Forward** to continue.To view the complete Errata Advisory text for an update, highlight the relevant package and click the **View Advisory** button. When finished, click **OK**.

Select those you wish to download and click **Forward** to continue.

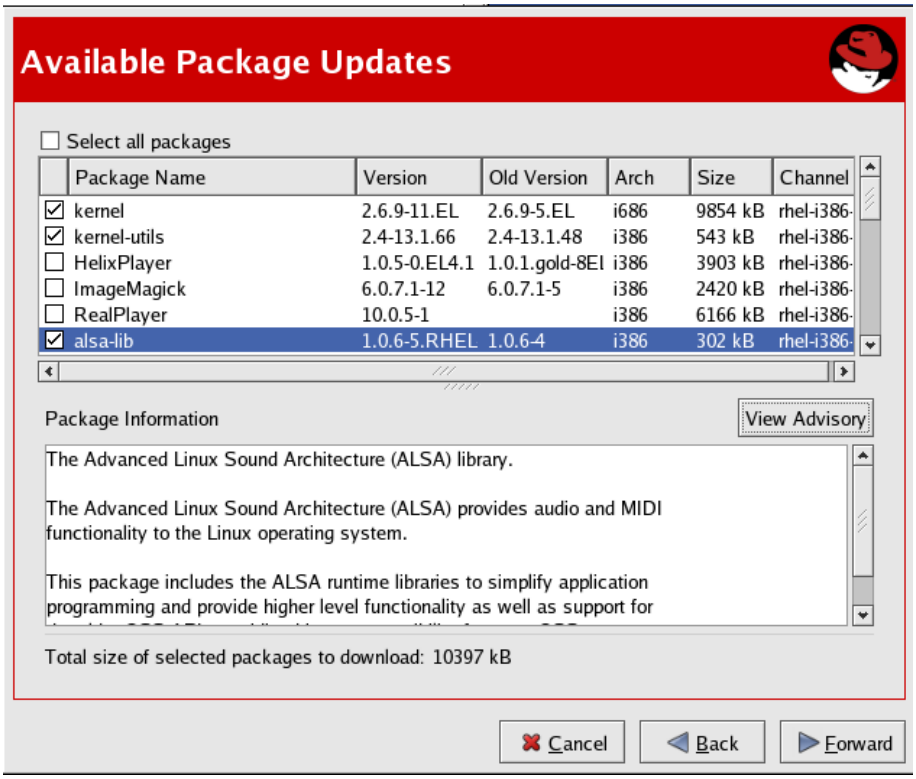
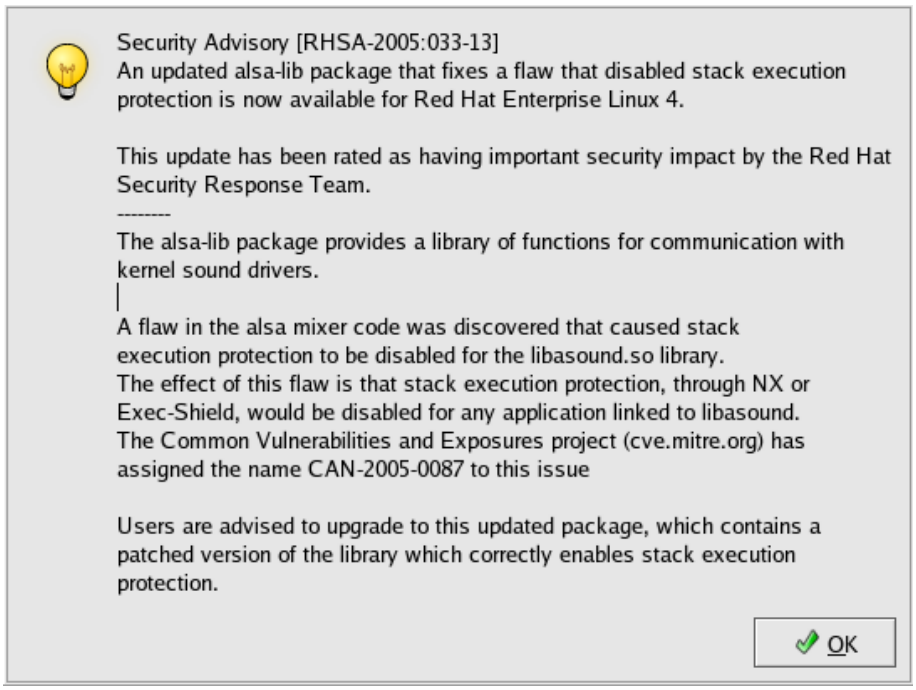

Available Package Updates
Select all packages
Package Name
Version
Old Version
Arch
Size
Channel
kernel 2.6.9-11.EL 2.6.9-5.EL i686 9854 kB rhel-i386-
kernel-utils 2.4-13.1.66 2.4-13.1.48 i386 543 kB rhel-i386-
HelixPlayer 1.0.5-0.EL4.1 1.0.1.gold-8El i386 3903 kB rhel-i386-
ImageMagick 6.0.7.1-12 6.0.7.1-5 i386 2420 kB rhel-i386-
RealPlayer 10.0.5-1 i386 6166 kB rhel-i386-
alsa-lib 1.0.6-5.RHEL 1.0.6-4 i386 302 kB rhel-i386-
Package Information
View Advisory
The Advanced Linux Sound Architecture (ALSA) library.
The Advanced Linux Sound Architecture (ALSA) provides audio and MIDI functionality to the Linux operating system.
This package includes the ALSA runtime libraries to simplify application programming and provide higher level functionality as well as support for
Total size of selected packages to download: 10397 kB
Cancel
Back
Forward

Figure 2.11. Available Package Updates


Security Advisory [RHSA-2005:033-13]
An updated alsa-lib package that fixes a flaw that disabled stack execution protection is now available for Red Hat Enterprise Linux 4.
This update has been rated as having important security impact by the Red Hat Security Response Team.

The alsa-lib package provides a library of functions for communication with kernel sound drivers.
A flaw in the alsa mixer code was discovered that caused stack execution protection to be disabled for the libasound.so library.
The effect of this flaw is that stack execution protection, through NX or Exec-Shield, would be disabled for any application linked to libasound.
The Common Vulnerabilities and Exposures project (cve.mitre.org) has assigned the name CAN-2005-0087 to this issue
Users are advised to upgrade to this updated package, which contains a patched version of the library which correctly enables stack execution protection.
OK

Figure 2.12. Example Errata Advisory

2.2.6. Retrieving Packages

The Red Hat Update Agent tests the packages you selected to be certain that the requirements of each RPM are met. If any additional packages are required, Red Hat Update Agent displays an error message. Click **OK** to continue.

Once all dependencies are met, Red Hat Update Agent retrieves the packages from RHN. As the packages are downloaded, they are temporarily stored in **/var/spool/up2date/**.

When all packages have been downloaded, click **Forward** to continue.

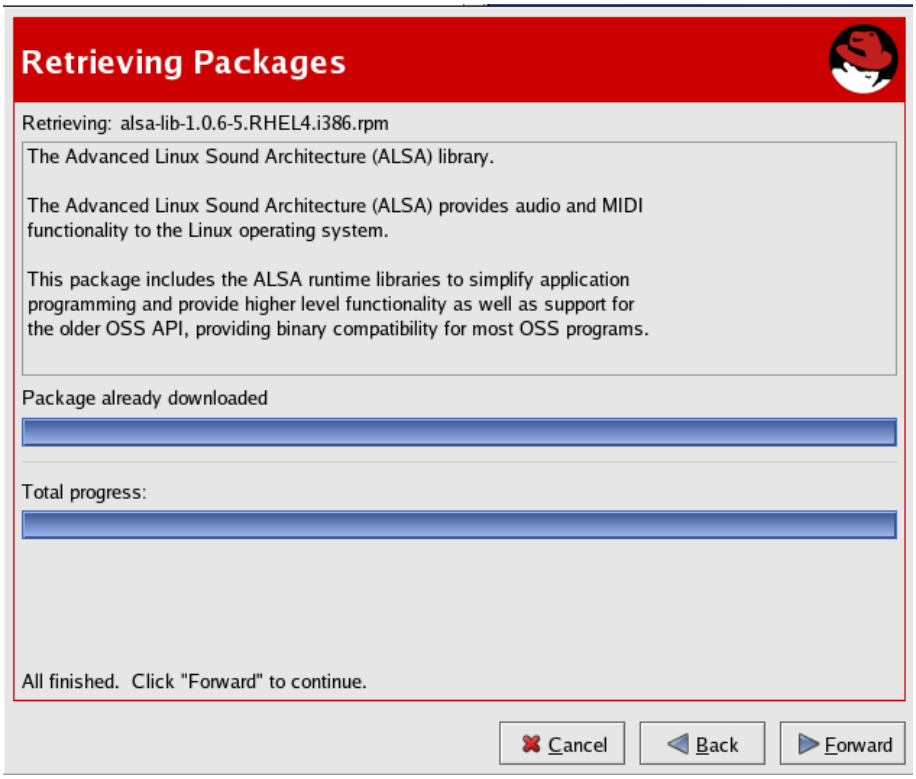

Retrieving Packages
Retrieving: alsa-lib-1.0.6-5.RHEL4.i386.rpm
The Advanced Linux Sound Architecture (ALSA) library.
The Advanced Linux Sound Architecture (ALSA) provides audio and MIDI functionality to the Linux operating system.
This package includes the ALSA runtime libraries to simplify application programming and provide higher level functionality as well as support for the older OSS API, providing binary compatibility for most OSS programs.
Package already downloaded
Total progress:
All finished. Click "Forward" to continue.
Cancel
Back
Forward

Figure 2.13. Retrieving Packages

2.2.7. Installing Packages

The packages must be installed after downloading them via the **Red Hat Update Agent**. If you chose not to install the packages via the **Red Hat Update Agent**, skip to Section 2.3.2, "Manual Package Installation" for further instructions. If you configured the Red Hat Update Agent to install the packages (the default setting), the installation process begins. The progress of installing each package, as well as the total progress, is displayed. When the packages have been installed, as seen in Figure 2.14, "Installing Packages", click **Forward** to continue.

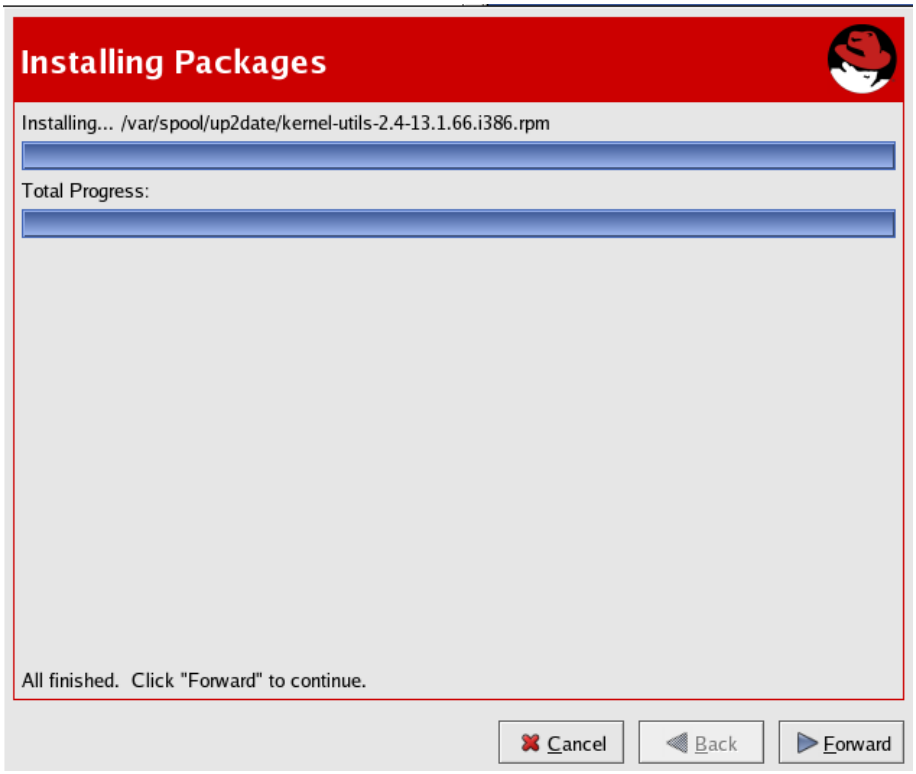


Figure 2.14. Installing Packages

When the **Red Hat Update Agent** has finished downloading the desired packages (and installing them if you chose the install option), it displays the screen in Figure 2.15, “All Finished”. Click **Finish** to exit the **Red Hat Update Agent**.

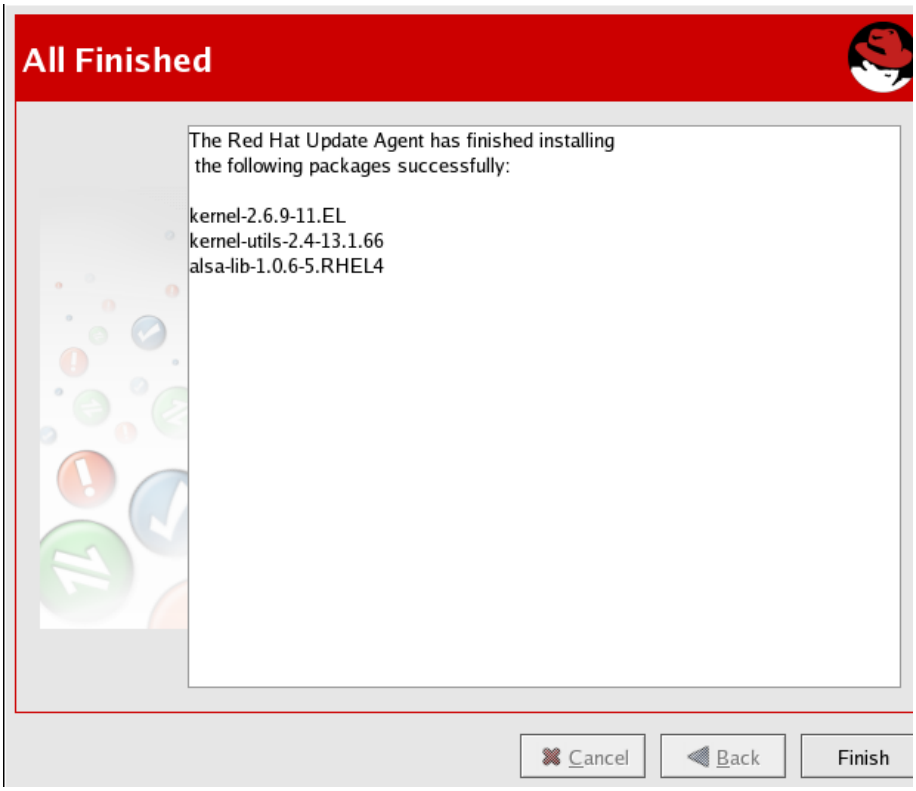


Figure 2.15. All Finished

2.3. Command Line Version

If you are not running X, you can still run the **Red Hat Update Agent** from a virtual console or remote terminal. If you are running X but want to use the command line version, you can force it not to display the graphical interface with the following command:

```
up2date --nox
```

The command line version of the **Red Hat Update Agent** allows you to perform advanced functions or to perform actions with little or no interaction. For example, the following command updates your system with no interaction. It downloads the newer packages and installs them if you configured it to do so.

```
up2date -u
```

The command line version of the **Red Hat Update Agent** accepts the following arguments:

Table 2.2. Update Agent Command Line Arguments

Option	Description
-?, **--usage**	Briefly describe the available options.
-h, **--help**	List the available options and exit.
--arch=*architecture*	Force **up2date** to install this architecture of the package. Not valid with **--update**, **--list**, or **--dry-run**.
--channel=*channel*	Specify from which channels to update using channel labels.
--configure	Configure **Red Hat Update Agent** options. Refer to Section 2.4, “Configuration” for detailed instructions.
-d, **--download**	Download packages only; do not install them. This argument temporarily overrides the configuration option **Do not install packages after retrieval.** Use this option if you prefer to install the packages manually.
--dbpath=*dir*	Specify an alternate RPM database to use temporarily.
--dry-run	Do everything but download and install packages. This is useful in checking dependencies and other requirements prior to actual installation.
-f, **--force**	Force package installation. This option temporarily overrides the file, package, and configuration skip lists.
--firstboot	Pop up in the center of the screen for Firstboot.
--get	Fetch the package specified without resolving dependencies.
--get-source	Fetch the source package specified without resolving dependencies.
--gpg-flags	Show the flags with which GPG is invoked, such as the keyring.
--hardware	Update this system's hardware profile on RHN.
-i, **--install**	Install packages after they are downloaded. This argument temporarily overrides the configuration option **Do not install packages after retrieval.**
--installall=<*channel-label*>	Install all available packages from a given channel
--justdb	Only add packages to the database and do not install them.
-k, **--packagedir**	Specify a colon-separated path of directories in which to look for packages before trying to download them.
-l, **--list**	List packages relevant to the system.
--list-rollbacks	Show the package rollbacks available.
--nodownload	Do not download packages at all. This is useful in testing.
--nosig	Do not use GPG to check package signatures. This option temporarily overrides the saved configuration option.
--nosrc	Do not download source packages (SRPMs).
--nox	Do not attempt to run in X. This launches the command line version of the **Red Hat Update Agent**.
-p, **--packages**	Update packages associated with this System Profile.
--proxy=*proxy URL*	Specify an HTTP proxy to use.

--proxyPassword=*proxy password*	Specify a password to use with an authenticated HTTP proxy.
--proxyUser=*proxy user ID*	Specify a username to use with an authenticated HTTP proxy.
--register	Register (or re-register) this system with RHN. Refer to Section 2.2, “Registration” for detailed instructions.
--serverUrl=*server URL*	Specify an alternate server from which to retrieve packages.
--showall	List all packages available for download.
--show-available	List all packages available that are not currently installed.
--show-channels	Show the channel name associated with each package.
--show-orphans	List all packages currently installed that are not in channels to which the system is subscribed.
--show-package-dialog	Show the package installation dialog in GUI mode.
--solvedeps=*dependencies*	Find, download, and install the packages necessary to resolve dependencies.
--src	Download source packages, as well as binary RPMs.
--tmpdir=*directory*	Temporarily override the configured package directory. The default location is **/var/spool/up2date**. This option is useful if you do not have enough space in the configured location.
-u, **--update**	Update system with all relevant packages.
--undo	Reverse the last package set update.
--upgrade-to-release=*release version*	Upgrade to the channel specified.
--uuid=*uuid*	Pass in a Unique User ID generated by the Alert Notification tool.
-v, **--verbose**	Show additional output while updating.
--version	Show **up2date** version information.
--whatprovides=*dependencies*	Show the packages that resolve the comma-separated list of dependencies.

Note

The **--solvedeps** and **--whatprovides** options can be used to solve the dependencies for an RPM regardless even if your system does not currently have access to a channel that contains that package.

2.3.1. Installing the Red Hat GPG key

The first time you run the graphical version of the **Red Hat Update Agent**, it prompts you to install the Red Hat GPG key. This key is required to authenticate the packages downloaded from Red Hat Network. If you run the command line version the first time you start **Red Hat Update Agent**, you must install the Red Hat GPG key manually. If you do not have it installed, you will see the following message:

```
Your GPG keyring does not contain the Red Hat, Inc. public key. Without it,
you will be unable to verify that packages Update Agent downloads are securely
signed by Red Hat.
```

Note

GPG keys must be installed for each user. To install the key to use with Red Hat Network, import the key while logged in as root.

The method for installing the key varies depending on your version of RPM. Starting with version 4.1, which shipped with Red Hat Enterprise Linux 3, you may use RPM to import GPG keys. Issue the following command at a shell prompt as root:

```
rpm --import /usr/share/doc/rpm-4.1/RPM-GPG-KEY
```

For older versions of RPM, such as the one that came with Red Hat Enterprise Linux 2.1, use the **gpg** command (as root):

```
/usr/bin/gpg --import /usr/share/rhn/RPM-GPG-KEY
```

To download the Red Hat GPG key first, you may obtain it from https://www.redhat.com/security/team/key.html . Here's an example:

```
 Type bits/keyID Date User ID pub 1024D/650D5882 2001-11-21 Red Hat, Inc.
(Security Response Team) sub 2048g/7EAB9AFD 2001-11-21 -----BEGIN PGP PUBLIC
KEY BLOCK----- Version: GnuPG v1.2.1 (GNU/Linux)
mQGiBDv70vQRBADh701rf8WUzDG88kqlV/N5KQ1PF0amnODB/1EeuAD7n6bCBRmV
ekQWJCdfab0Rf1S+VsFg6IAAAmDIarVnacTLQzqCdGJqTpXm/rGVpLv+mCh+OmT9
QRFbjSzB0uPJOpiIvJwSS00D/wJ8XKzHkVNgW3DiJ9Qz2BHYszU2ISI6FwCgxY6d
IVjWT5jblkLNjtD3+fR024ED/i0e2knetTX3S9LjC+HdGvP8Eds92Ti2CnJLaFJk
Rp749PucnK9mzxPcO2jSHgdtjWAXst/st+gWFVbFmkjBQDVSd00B/xEwI1T1+LN8
V7R8BElBmg99IlJmDvA2BI/seXvafhzly9bxSHScFnceco/Az9umIs3NXwv3/yOm
ZakDBAC6SAGHBmpVkOdeXJDdb4LcbEhErFU3CpRCjZ6AOnFuiV1MGdulZXvEUgBA
I6/PDE5nBHfZY3zPjyLPZVtgYioJpZqcRIx/g+bX2O8kPqvJEuZ19tLCdykfZGpy
bsV7QdSGqBk3snNOizmFj543RaHyEbnwKWbNADhujWMeUAxN+7Q8UmVkIEhhdCwg
SW5jLiAoU2VjdXJpdHkgUmVzcG9uc2UgVGVhbSkgPHNlY2FsZXJ0QHJlZGhhdC5j
b20+iFcEExECABcFAj3GczYFCwcKAwQDFQMCAxYCAQIXgAAKCRBeVICDZQ1YghAU
AJoCeQfuMR2dKyLft/10O6qUs+MNLQCggJgdO8MUO2y11TWID3XOYgyQG+2InAQT
AQIABgUCPtyYpQAKCRDurUz9SaVj2e97A/0b2s7OhhAMljNwMQS4I2UWVGbgtxdu
D+yBcG/3mwL76MJVY7aX+NN/tT9yDGU+FSiQZZCL/4OFOHMvjpcDqfJY+zpTlBii
ZMAPJWTs2bB+0QaXxUgWlwW84GVf2rA6RSbvMLTbDjTH8t7J1RGP9zAqu8SgraTA
QbQdao6TNxVt+ohGBBMRAgAGBQI+3LjCAAoJECGRgM3bQqYOf5MAoIjiJDe+hDOj
9+jlR0qDs9lIi/C2AJ9SBBfd4A8hyR4z3lY7e0LzjWF51LkCDQQ7+9O3EAgA8tMs
xdUmuTfA+X78fMXh7LCvrL4Hi28CqvNM+Au81XJjDLNawZvpVmFlMmd9h0Xb5Jt2
BZWLR13rcDUByNdw1EWhVAzCz6Bp9Z3MIDhcP00iIBctIHn7YP9fi5vV0G03iryT
XE01mhWoBlC233wr3XHwsqxFfZzaCZqqNKTl0+PNfEAIzJRgtYiW8nzFTPpIR05E
oRn6EvmQfayOF2uYDX9Sk//lOD7T7RLtKjM/hPW/9NoCGwwROaG+VUzVv4aelh1L
dJGEjpFtdxcrOUMD8xbkuGMznu0mpDI+J2BUDh5n57yOyEMaGrQ0jfY1ZqdqDvZg
osY1ZHa6KlmuCWNTnwADBQf/XYhCicp6iLetnPv6lYtyRfFRpnK98w3br+fThywC
t81P2nKv8lio6OsRbksGc1gX8Zl6GoHQYfDe7hYsCHZPoWErobECFds5E9M7cmzV
TTyNTvrELrs07jyuPb4Q+mHcsYPILGR3M+rnXKGjloz+05kOPRJaBEBzP6B8SZKy
QNqEfTkTYU4Rbhkzz/UxUxZoRZ+tqVjNbPKFpRraiQrUDsZFbgksBCzkzd0YURvi
CegO2K7JPKbZJo6eJA10qiBQvAx2EUijZfxIKqZeLx40EKMaL7Wa2CM/xmkQmCgg
Hyu5bmLSMZ7cxFSWyXOst78dehCKv9WyPxHV3m4iANWFL4hGBBgRAgAGBQI7+9O3
AAoJEF5UgINlDViCKWcAoMCeYStWVKXJTytzHEL6Wl8rXr8WAKCHuapJIA4/eFsf
4ciWtjY8cO0v8Q== =yOVZ -----END PGP PUBLIC KEY BLOCK-----
```

Save the text file and import it into your keyring using the method applicable to your version of RPM.

2.3.2. Manual Package Installation

If you chose to download, but not install, the software updates with the **Red Hat Update Agent** or from the RHN website, you must install them manually using RPM.

To install them, change to the directory that contains the downloaded packages. The default directory is **/var/spool/up2date**. Type the command **rpm -Uvh *.rpm**. When the packages finish installing, you can delete them if you wish. You do not need them anymore.

After installing the packages, you must update your System Profile so that you are not prompted to download them again. Refer to Section 2.3.3, “Synchronizing Your System Profile” for details.

2.3.3. Synchronizing Your System Profile

If you configured the **Red Hat Update Agent** to install the latest packages, the System Profile stored by Red Hat Network is updated after the packages are installed. However, if you only download the latest RPM packages using the **Red Hat Update Agent**, download the RPM packages from the website, or upgrade/install/remove RPM packages yourself, your System Profile is not updated automatically. You must send your updated System Profile to the RHN Servers.

To synchronize the RPM package list on your local system and on Red Hat Network, run the command:

```
up2date -p
```

After running this command, your RHN System Profile reflects the latest software versions installed on your system.

2.3.4. Log File

The **Red Hat Update Agent** keeps a log of all the actions that it performs on your system in the file **/var/log/up2date**. It uses the standard rotating log method. Thus, older logs are in **/var/log/up2date.1**, **/var/log/up2date.2**, and **/var/log/up2date.3**. The log files store actions performed by the **Red Hat Update Agent** such as when your RPM database is opened, when it connects to Red Hat Network to retrieve information from your System Profile, which packages are downloaded, which packages are installed using the **Red Hat Update Agent**, and which packages are deleted from your system after installation. If you choose to install and delete packages yourself, it is not logged in this file. Red Hat Network recommends that you keep a log of actions not performed with the **Red Hat Update Agent**.

2.4. Configuration

The **Red Hat Update Agent** offers various options to configure its settings.

If you are not running the X Window System or prefer the command line version, skip to Section 2.4.2, “Command Line Version”.

2.4.1. Using the Red Hat Update Agent Configuration Tool

You must be root to run the **Red Hat Update Agent Configuration Tool**. If started by a user other than root, the Red Hat Update Agent prompts you for the root password. The **Red Hat Update Agent Configuration Tool** can be started by typing the command **up2date --config** at a shell prompt (for example, an **xterm** or a **gnome-terminal**).

2.4.1.1. General Settings

The **General** tab allows you to enable an HTTP Proxy Server. If your network connection requires you to use an HTTP Proxy Server to make HTTP connections, select the **Enable HTTP Proxy** option and type your proxy server in the text field with the format http://HOST:PORT. For example, to use the proxy server squid.mysite.org on port 3128, you would enter **squid.mysite.org:3128** in the text field. Additionally, if your proxy server requires a username and password, select the **Use Authentication** option and enter your username and password in the respective text fields.

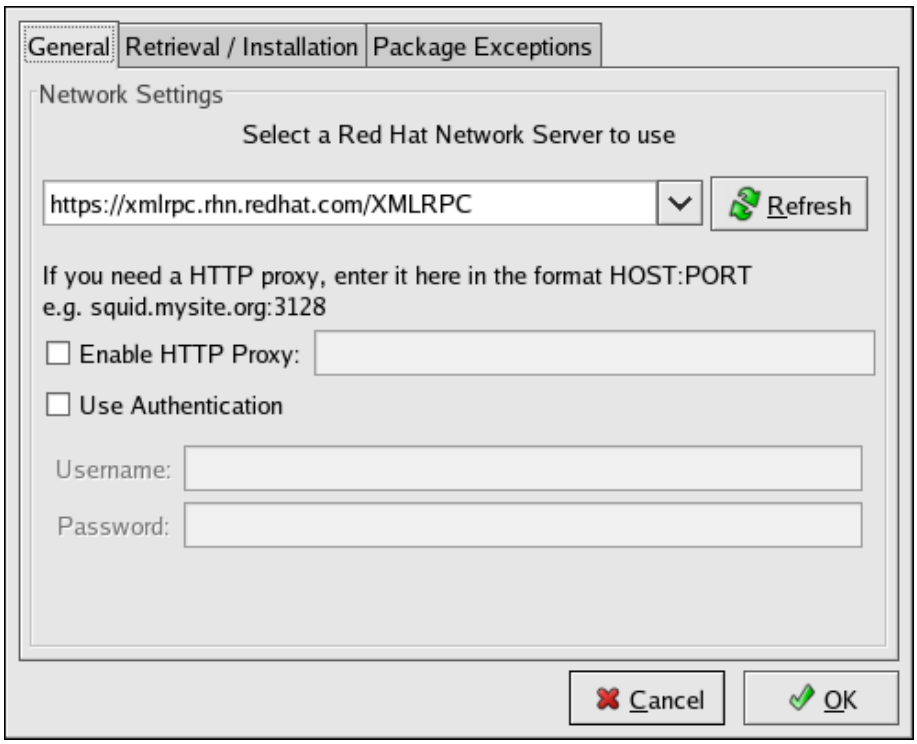


Figure 2.16. General Settings

In addition, RHN Proxy and Satellite customers have the option of selecting Red Hat Network Servers here. These customers should refer to the *RHN Client Configuration Guide* for detailed instructions.

2.4.1.2. Retrieval/Installation Settings

The **`Retrieval/Installation`** tab allows you to customize your software package retrieval and package installation preferences.

Warning

You must use **Red Hat Update Agent** Version 2.5.4 or higher to upgrade your kernel automatically. **Red Hat Update Agent** will install the updated kernel and configure LILO or GRUB to boot the new kernel the next time the system is rebooted.

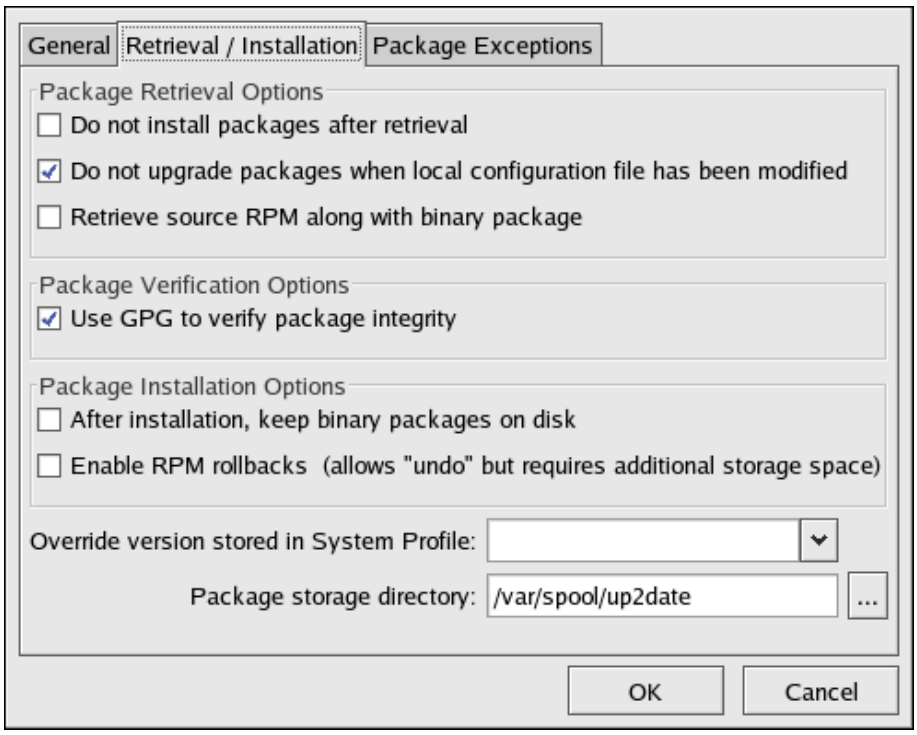

General
Retrieval / Installation
Package Exceptions
Package Retrieval Options
Do not install packages after retrieval
Do not upgrade packages when local configuration file has been modified
Retrieve source RPM along with binary package
Package Verification Options
Use GPG to verify package integrity
Package Installation Options
After installation, keep binary packages on disk
Enable RPM rollbacks (allows "undo" but requires additional storage space)
Override version stored in System Profile:
Package storage directory:
/var/spool/up2date
...
OK
Cancel

Figure 2.17. Retrieval/Installation Settings

The following package retrieval options can be selected (see Figure 2.17, "Retrieval/Installation Settings"):

- **Do not install packages after retrieval** — download selected RPM packages to the desired directory and ignore the installation preferences
- **Do not upgrade packages when local configuration file has been modified** — if the configuration file has been modified for a package such as **`apache`** or **`squid`**, do not attempt to upgrade it. This option is useful if you are installing custom RPMs on your system and you do not want them updated or reverted to the default Red Hat Enterprise Linux packages.
- **Retrieve source RPM along with binary package** — download both the source (**`*.src.rpm`**) and the binary (**`*.[architecture].rpm`**) files

The following installation options are configurable (see Figure 2.17, "Retrieval/Installation Settings"):

- **Use GPG to verify package integrity** — before installing packages, verify Red Hat's GPG signature (highly recommended for security reasons)
- **After installation, keep binary packages on disk** — save binary packages in the desired directory instead of deleting them after installation

The following additional options are configurable from this tab:

- **Override version stored in System Profile** — override the Red Hat Linux version in your System Profile
- **Package storage directory** — change the directory where packages are downloaded; the default location is **`/var/spool/up2date/`**

2.4.1.3. Package Exceptions Settings

The **`Package Exceptions`** tab allows you to define which packages to exclude from the list of

updated RPM packages according to the package name or file name (see Figure 2.18, “Package Exceptions Settings”).

To define a set of packages to be excluded according to the package name, enter a character string including wild cards (*) in the **Add new** text field under in the **Package Names to Skip** section heading. A wild card at the end of the character string indicates that all packages beginning with the character string are excluded from the list. A wild card at the beginning of the character string indicates that any packages that end with the character string are excluded from the list.

For example, if the string **kernel*** is in the **Package Names to Skip** section, the **Red Hat Update Agent** will not display any packages beginning with kernel.

To exclude packages by file name, apply the same rules to the field below **File Names to Skip** section heading.

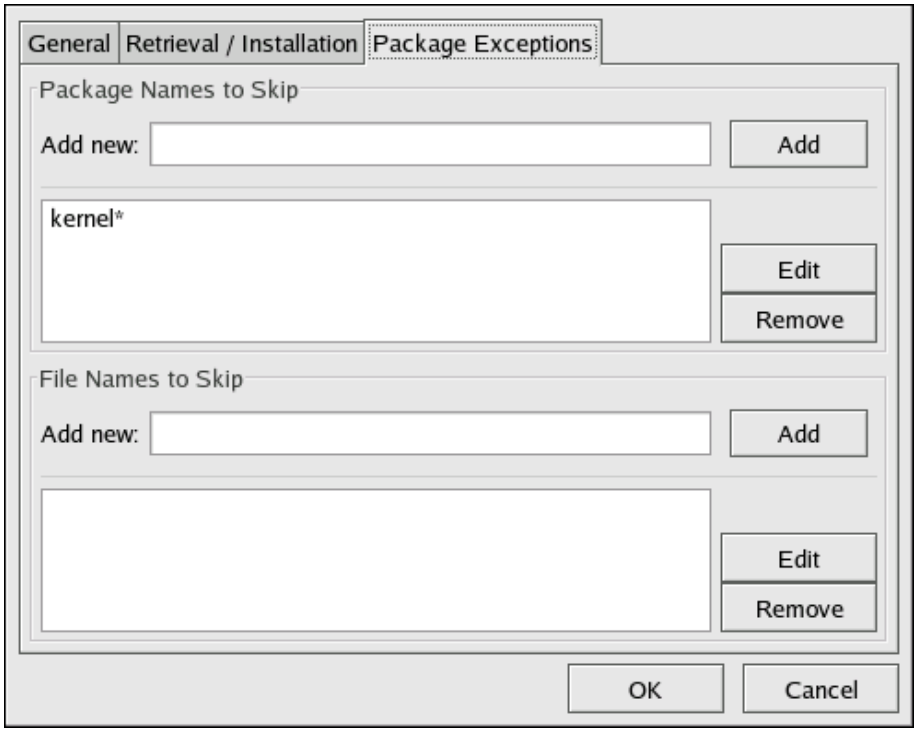


Figure 2.18. Package Exceptions Settings

2.4.2. Command Line Version

The command line version of this tool performs the same function as the graphical version. It allows you to configure the settings used by the **Red Hat Update Agent** and store them in the configuration file **/etc/sysconfig/rhn/up2date**.

To run the command line version of the **Red Hat Update Agent Configuration Tool**, use the following command:

```
up2date --nox --configure
```

You are presented with a list of options and their current values:

```
 0. debug No 1. isatty Yes 2. depslist [] 3. networkSetup Yes 4. retrieveOnly
No 5. enableRollbacks No 6. pkgSkipList ['kernel*'] 7. storageDir
/var/spool/up2date 8. adminAddress ['root@localhost'] 9. noBootLoader No 10.
serverURL https://xmlrpc.rhn.redhat.com/XMLRPC 11. fileSkipList [] 12.
sslCACert /usr/share/rhn/RHNS-CA-CERT 13. noReplaceConfig Yes 14.
useNoSSLForPackage No 15. systemIdPath /etc/sysconfig/rhn/systemid 16.
enableProxyAuth No 17. retrieveSource No 18. versionOverride 19.
headerFetchCount 10 20. networkRetries 5 21. enableProxy No 22. proxyPassword
23. noSSLServerURL http://xmlrpc.rhn.redhat.com/XMLRPC 24. keepAfterInstall No
25. proxyUser 26. removeSkipList ['kernel*'] 27. useGPG Yes 28. gpgKeyRing
/etc/sysconfig/rhn/up2date-keyring.gpg 29. httpProxy 30. headerCacheSize 40
31. forceInstall No Enter number of item to edit <return to exit, q to quit
without saving>:
```

Enter the number of the item to modify and enter a new value for the option. When you finish changing your configuration, press **Enter** to save your changes and exit. Press **q** and then **Enter** to quit without saving your changes.

Important

Although this is not configurable, users should still make note that the port used by the **Red Hat Update Agent** is 443 for SSL (HTTPS) and 80 for non-SSL (HTTP). By default, **up2date** uses SSL only. For this reason, users should ensure that their firewalls allow connections over port 443. To bypass SSL, change the protocol for serverURL from **https** to **http** in the **/etc/sysconfig/rhn/up2date** configuration file.

2.5. Registering with Activation Keys

In addition to the standard **Red Hat Update Agent** interface, **up2date** offers a utility aimed at batch processing system registrations: activation keys. Each unique key can be used to register Red Hat Enterprise Linux systems, entitle them to an RHN service level, and subscribe them to specific channels and system groups, all in one action. This automation bypasses entitlement and registration via Red Hat Network Registration Client and Red Hat Update Agent.

Alternatively, both the Red Hat Network Registration Client and Red Hat Update Agent offer the activation keys utility **rhnreg_ks** as part of their packages.

Note

Systems running Red Hat Enterprise Linux 2.1 need version 2.9.3-1 or higher of the **rhn_register** package. It is highly recommended that you obtain the latest version before using activation keys.

Before using an activation key you must first generate one through the RHN website. Refer to Section 6.4.6, “Activation Keys — ” for precise steps.

To use an activation key, run the following command as root from a shell prompt on the system to be registered:

```
rhnreg_ks --activationkey=7202f3b7d218cf59b764f9f6e9fa281b
```

The precise value of the activation key varies.

Systems running Red Hat Enterprise Linux 2.1 substitute the **--serialnumber** option for the **--activationkey** option:

```
rhnreg_ks --serialnumber=7202f3b7d218cf59b764f9f6e9fa281b
```

In addition, Provisioning-entitled systems may use multiple activation keys at once, either at the command line or within kickstart profiles. This allows Administrators to include a variety of values without creating a special key for the desired results. To do this, specify the keys separated by commas, like this:

```
rhnreg_ks --activationkey=7202f3b7d218cf59b764f9f6e9fa281b,\
39f41081f0329c20798876f37cb9p6a3
```

Note

The trailing backslash (\) in this command example is a continuation character; it may safely be omitted.

Refer to Section 6.4.6.2, “Using Multiple Activation Keys at Once — ” to understand how differences in activation keys are handled.

The above command performs all the actions of the **Red Hat Network Registration Client** and the registration function of the **Red Hat Update Agent**. Do not run either of these applications for registration after running **rhnreg_ks**.

A System Profile, including software and hardware information, is created for the system and sent to the RHN Servers along with the unique activation key. The system is registered with RHN under the account used to generate the key, entitled to an RHN service offering, and subscribed to the RHN channels and system groups selected during key generation. The system is not subscribed to channels that contain packages unsuitable for the system. For example, a Red Hat Enterprise Linux 2.1 system cannot be subscribed to the Red Hat Enterprise Linux 3 channel.

The unique Digital Certificate for the system is generated on the system in the file **/etc/sysconfig/rhn/systemid**.

When using activation keys to assign channels, consider these rules:

- A key may specify either zero or one base channel. If specified, it must be a custom base channel. If not, the base channel corresponding to the system's Red Hat distribution is chosen. For instance, you may not subscribe a Red Hat Enterprise Linux 2.1 system to the Red Hat Enterprise Linux 3 channel.
- A key may specify any number of child channels. For each child channel, subscription is attempted. If the child channel matches the system's base channel, subscription succeeds. If it does not, the subscription fails silently. Refer to Section 6.6, “Channels” for more information.
- Keys may be modified by any user with the role of Activation Key Administrator or Organization Administrator (or both). These permissions are set through the **Users** tab of the RHN website. Refer

to Section 6.8, “Users — ” for details.

- Systems registered by activation keys are tied to the organization account in which the key was created, not the key itself. After registration, a key can be deleted safely without any effect on the systems it was used to register.

Chapter 3. Red Hat Network Daemon

The Red Hat Network Daemon (**rhnsd**) periodically connects to Red Hat Network to check for updates and notifications. The daemon, which runs in the background, is typically started from the initialization scripts in **/etc/init.d/rhnsd** or **/etc/rc.d/init.d/rhnsd**.

Tip

Provisioning-entitled systems served by an RHN Satellite may have actions immediately initiated or *pushed* to them. Refer to Section 6.4.2.9.1, “System Details ⇒ Details” for instructions on enabling this feature.

To check for updates, **rhnsd** runs an external program called **rhn_check** located in **/usr/sbin/**. This is a small application that makes the network connection to RHN. The Red Hat Network Daemon does not listen on any network ports or talk to the network directly. All network activity is done via the **rhn_check** utility.

3.1. Configuring

The Red Hat Network Daemon can be configured by editing the **/etc/sysconfig/rhn/rhnsd** configuration file. This is actually the configuration file the **rhnsd** initialization script uses. The most important setting offered by the daemon is its check-in frequency. The default interval time is four hours (240 minutes). If you modify the configuration file, you must (as root) restart the daemon with the command **service rhnsd restart** or **/etc/rc.d/init.d/rhnsd restart**.

Important

The minimum time interval allowed is one hour (60 minutes). If you set the interval below one hour, it will default to four hours (240 minutes).

3.2. Viewing Status

You can view the status of the **rhnsd** by typing the command **service rhnsd status** or **/etc/rc.d/init.d/rhnsd status** at a shell prompt.

3.3. Disabling

To disable the daemon, (as root) run the **ntsysv** utility and uncheck **rhnsd**. You can also (as root) execute the command **chkconfig rhnsd off**. Using these two methods only disables the service the next time the system is started. To stop the service immediately, use the command **service rhnsd stop** or **/etc/rc.d/init.d/rhnsd stop**.

3.4. Troubleshooting

If you see messages indicating that checkins are not taking place, the RHN client on your system is not successfully reaching Red Hat Network. Make certain:

- your client is configured correctly.
- your system can communicate with RHN via SSL (port 443). You may test this by running the following command from a shell prompt:

```
telnet xmlrpc.rhn.redhat.com 443
```

- the Red Hat Network Daemon is activated and running. You may ensure this by running the following commands:

```
chkconfig --level 345 rhnsd on
```

```
service rhnsd start
```

If these are correct and your systems still indicate they are not checking in, please contact our technical support team.

Chapter 4. Red Hat Network Alert Notification Tool

The **Red Hat Network Alert Notification Tool** is a notifier that appears on the panel and alerts users when software package updates are available for their systems. The list of updates is retrieved from the RHN Servers. The system does not have to be registered with Red Hat Network to display a list of updates; however, retrieving the updates with the **Red Hat Update Agent** requires registration with Red Hat Network and a subscription to an RHN service offering. The notifier does not send any identifiable information about the user or the system to the RHN Servers.

To use the **Red Hat Network Alert Notification Tool**, you must install the **`rhn-applet`** RPM package and use the X Window System.

Starting with Red Hat Enterprise Linux 3, the **Red Hat Network Alert Notification Tool** appears on the panel by default as shown in Figure 4.1, “GNOME Panel with Red Hat Network Alert Notification Tool”.

Figure 4.1. GNOME Panel with Red Hat Network Alert Notification Tool

If it does not appear on the panel, you can add it:

- In Red Hat Enterprise Linux 3 and later, select Applications (the main menu on the panel) => **System Tools** => **Red Hat Network Alert Icon**. To ensure the icon appears on subsequent sessions, select the **`Save current setup`** checkbox when logging out.
- In Red Hat Enterprise Linux 2.1, select the **Main Menu Button** => **Panel** => **Add to Panel** => **Applet** => **Red Hat Network Monitor**. To move it around the panel, right-click on the applet, select **Move**, move the mouse left and right until it is in the desired location, and click the mouse to place the applet.

4.1. Configuring the Applet

The first time the **Red Hat Network Alert Notification Tool** is run, a configuration wizard starts. It displays the terms of service and allows the user to configure an HTTP proxy as shown in Figure 4.2, “HTTP Proxy Configuration”.

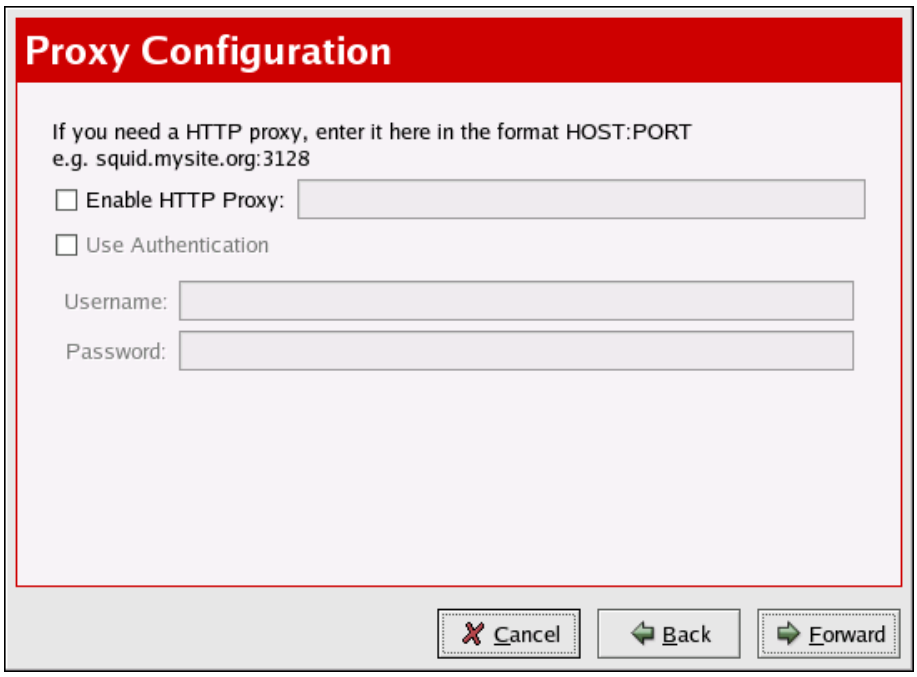


Figure 4.2. HTTP Proxy Configuration

If your network connection requires you to use an HTTP Proxy Server to make HTTP connections, on the **Proxy Configuration** screen, type your proxy server in the text field with the format HOST:PORT. For example, to use the proxy server http://squid.mysite.org on port 3128, enter **squid.mysite.org:3128** in the text field. Additionally, if your proxy server requires a username and password, select the **Use Authentication** option and enter your username and password in the respective text fields.

Tip

To run the configuration wizard again, right-click on the applet, and select **Configuration**.

Your preferences are written to the **.rhn-applet.conf** file in your home directory. The **Red Hat Network Alert Notification Tool** also uses the system-wide configuration file **/etc/sysconfig/rhn/rhn-applet**. The setting for **server_url** should be set to your satellite server. For example:

```
server_url=http://YourRHN_Satellite.com/APPLET
```

Or, for SSL:

```
server_url=https://YourRHN_Satellite.com/APPLET
```

You can also configure the **Red Hat Network Alert Notification Tool** to ignore specific packages. To select these packages, click on the applet and select the **Ignored Packages** tab.

4.2. Notification Icons

The applet displays a different icon, depending on the status of the updates. Table 4.1, “Red Hat

Network Alert Notification Tool Icons" shows the possible icons and their meaning.

Table 4.1. Red Hat Network Alert Notification Tool Icons

Icon	Description
	Updates are available
	System is up-to-date
	Checking for updates
	Error has occurred

If you see the icon, it is strongly recommended that you apply the updates. Refer to Section 4.4, "Applying Updates" for information on applying updates.

If you have scheduled updates to be installed, you can watch the applet icon to determine when updates are applied. The icon changes to the icon after the Errata Updates are applied.

If you apply a kernel update (or the kernel update is automatically applied), the applet displays the icon until the system is rebooted with the new kernel. If you double-click on the applet, the **Available Updates** tab displays a list of packages that can be updated on your system.

4.3. Viewing Updates

Clicking on the **Red Hat Network Alert Notification Tool** displays a list of available updates. To alter your list of excluded packages, click the **Ignored Packages** tab and make your modifications.

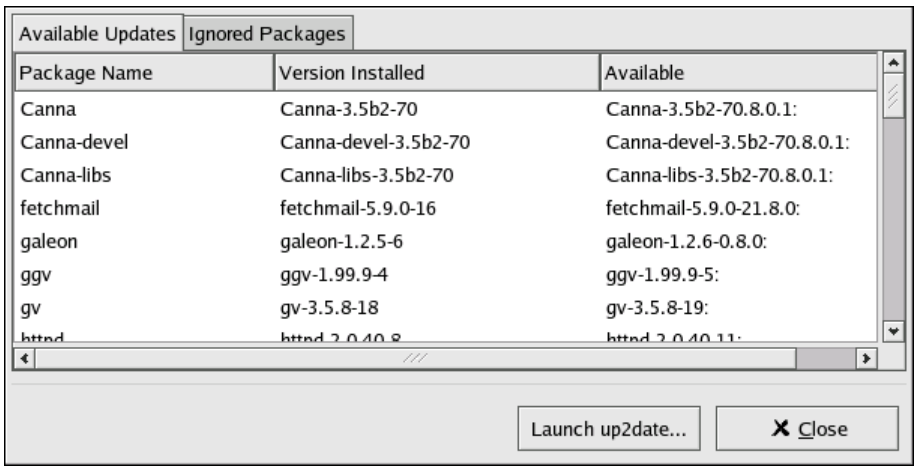


Figure 4.3. Available Updates

4.4. Applying Updates

If the system is registered with RHN and entitled to a service offering, you can apply the Errata Updates with the **Red Hat Update Agent**. To launch the **Red Hat Update Agent**, click on the applet, and then click on the **Launch up2date** button. You can also right-click on the icon and select **Launch up2date**. For more information on the **Red Hat Update Agent**, refer to Chapter 2, ***Red Hat Update Agent***.

4.5. Launching the RHN Website

The simplest way to obtain a comprehensive view of your system's status is to access the RHN website. This can be accomplished through the **Red Hat Network Alert Notification Tool** by right-clicking on it and selecting **RHN Website**. For more information on the RHN website, refer to Section 6.1, “Navigation”.

Chapter 5. Red Hat Network Registration Client

Before you begin using Red Hat Network, you must create a username, password, and System Profile. The **Red Hat Network Registration Client** walks you through this process.

Warning

Only systems running Red Hat Enterprise Linux 2.1 need to use the **Red Hat Network Registration Client** before starting the **Red Hat Update Agent**. Systems running Red Hat Enterprise Linux 3 and later have this registration functionality built into the **Red Hat Update Agent**. After registering your system, refer to Chapter 2, ***Red Hat Update Agent*** for instructions on starting the **Red Hat Update Agent**.

5.1. Configuring the Red Hat Network Registration Client

To start the graphical interface for configuring the application to connect through an HTTP proxy server, type the following command at a shell prompt:

```
rhn_register --configure
```

The window shown in Figure 5.1, “Red Hat Network Registration Client Configuration” appears.

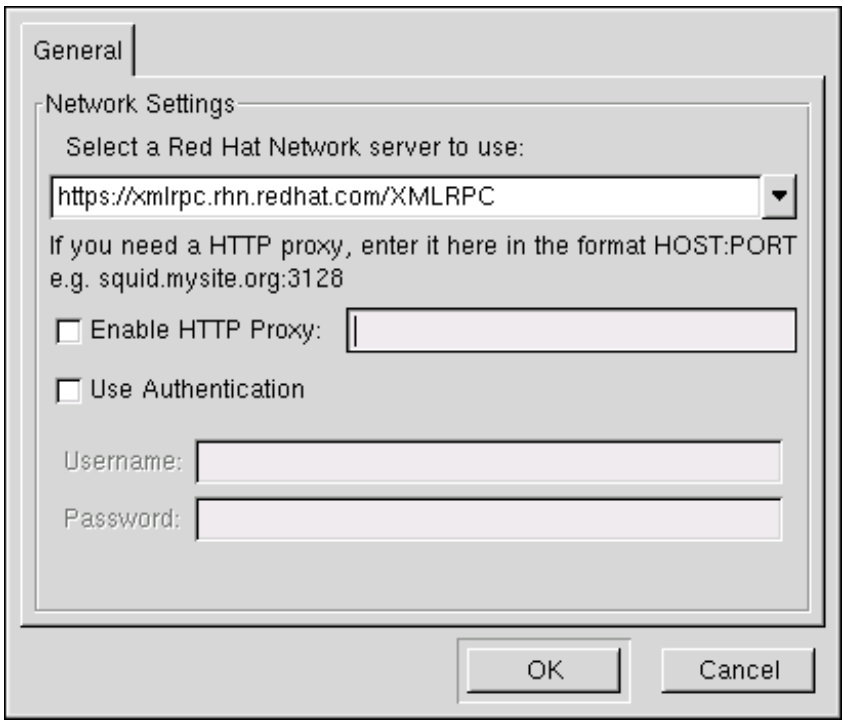


Figure 5.1. Red Hat Network Registration Client Configuration

To start the command line version, use the command:

```
rhn_register --nox --configure
```

It has more configuration options than the graphical version.

You will be presented with a list of options and their current values:

```
 0. enableProxyAuth No 1. noSSLServerURL http://xmlrpc.rhn.redhat.com/XMLRPC
2. oemInfoFile /etc/sysconfig/rhn/oeminfo 3. enableProxy No 4. networkSetup
Yes 5. httpProxy 6. proxyUser 7. serverURL
https://xmlrpc.rhn.redhat.com/XMLRPC 8. proxyPassword 9. debug No Enter number
of item to edit <return to exit, q to quit without saving>:
```

Enter the number of the item to modify and enter a new value for the option. When finished changing your configuration, press **Enter** to save your changes and exit. Press **q** and then **Enter** to quit without saving your changes.

The most common options configured are **enableProxy** and **httpProxy** to enable a proxy server. To enable a proxy server, change the value for **enableProxy** to **Yes** and the value of **httpProxy** to the name of the proxy server and port number in the format HOST:PORT. For example, to use the proxy server squid.mysite.org on port 3128, you would change the value to **squid.mysite.org:3128**.

If you require a proxy username and password, set **enableProxyAuth** to **Yes** to enable username/password authentication for the proxy, and set **proxyUser** and **proxyPassword** to the appropriate username and password for the proxy.

To bypass SSL, change the protocol for **serverURL** from **https** to **http** in the **/etc/sysconfig/rhn/rhn_register** file.

5.2. Starting the Red Hat Network Registration Client

You must be root to register a system with RHN. If started by a standard users, the **Red Hat Network Registration Client** prompts you to enter the root password before proceeding.

Important

If your username is part of a larger organizational account, be cautious when registering your systems. By default, all systems registered with the **Red Hat Network Registration Client** end up in the Ungrouped section of systems visible only to Organization Administrators. To ensure that you retain management of these systems, Red Hat recommends that your organization create an activation key associated with a specific system group and grant you permissions to that group. You may then register your systems using that activation key and find those System Profiles within RHN immediately. Refer to Section 2.5, “Registering with Activation Keys” for instructions.

To start the **Red Hat Network Registration Client**, use one of the following methods:

1. On the GNOME desktop, go to Applications (the main menu on the panel) => **Programs** => **System** => **Red Hat Network**
2. On the KDE desktop, go to Applications (the main menu on the panel) => **System** => **Red Hat Network**
3. Type the command **rhn_register** at a shell prompt (for example an **XTerm** or **GNOME terminal**)
4. If you are not running the X Window System, type the command **rhn_register** at a shell prompt. Refer to Section 5.7, “Text Mode RHN Registration Client” for further details.

Caution

You must use **Python 1.5.2-24** or later with Secure Sockets Layer (SSL) support. If not, the information transferred is not encrypted. If you have an earlier version of Python, you will see the message shown in Figure 5.2, "Use Python 1.5.2-24 or later". To determine the version of Python on your system, use the command **`rpm -q python`**. It is strongly recommended that you use **Python 1.5.2-24** or later.

Your system libraries do not support SSL (secure) connections. Any data that you send or receive from redhat.com will be transmitted in the clear. Continue anyway?
Yes
No

Figure 5.2. Use Python 1.5.2-24 or later

If you have already registered your system and try to register it again, the dialog box shown in Figure 5.3, "Warning: This System Already Registered" appears. If you continue, it overwrites your existing Digital Certificate file (**`/etc/sysconfig/rhn/systemid`**), and creates a different System Profile. You will no longer be able to use your previous System Profile — be sure this is what you want to do before you choose **`Yes`**.

If you overwrite an existing system registration, you can delete the unused profile via the website at https://rhn.redhat.com.

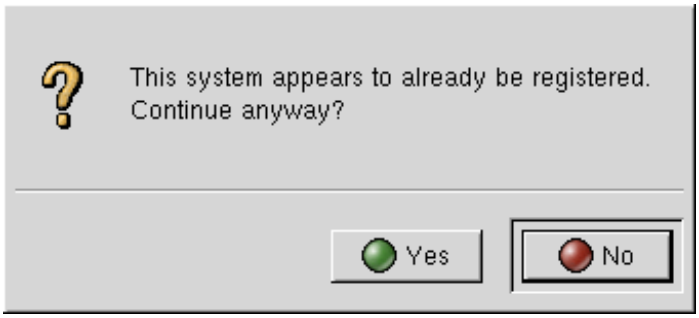


Figure 5.3. Warning: This System Already Registered

The opening screen for the **Red Hat Network Registration Client** provides a brief overview of the services available and the steps required to register (see Figure 5.4, "Welcome Screen"). Click **`Next`** to continue with the registration process. If you click **`Cancel`**, the registration process ends and no information is sent.

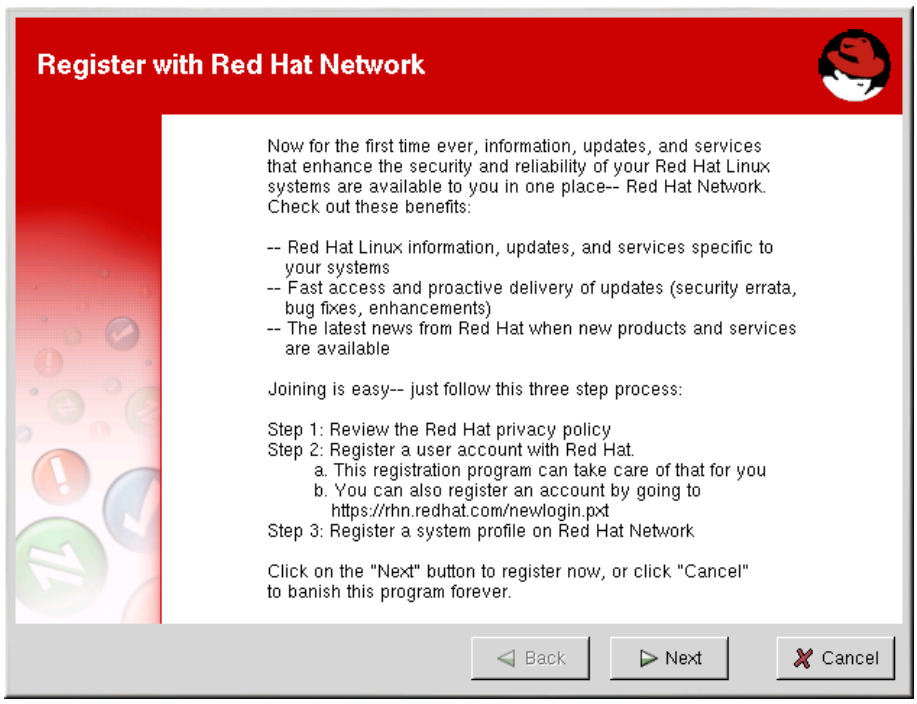

Register with Red Hat Network
Now for the first time ever, information, updates, and services that enhance the security and reliability of your Red Hat Linux systems are available to you in one place-- Red Hat Network. Check out these benefits:
-- Red Hat Linux information, updates, and services specific to your systems
-- Fast access and proactive delivery of updates (security errata, bug fixes, enhancements)
-- The latest news from Red Hat when new products and services are available
Joining is easy-- just follow this three step process:
Step 1: Review the Red Hat privacy policy
Step 2: Register a user account with Red Hat.
a. This registration program can take care of that for you
b. You can also register an account by going to https://rhn.redhat.com/newlogin.pxt
Step 3: Register a system profile on Red Hat Network
Click on the "Next" button to register now, or click "Cancel" to banish this program forever.
Back
Next
Cancel

Figure 5.4. Welcome Screen

Red Hat is committed to protecting your privacy (see Figure 5.5, “Red Hat Privacy Statement”). The information gathered during the Red Hat Network registration process is used to create a System Profile. The System Profile is essential if you wish to receive update notifications about your system.

Step 1: Review the Red Hat Privacy Statement
Privacy Statement
When it comes to your privacy, our promise is simple. Your personal information is yours, not ours. In fact, we feel so strongly about it that we encourage you to read our complete privacy policy below, so that you are comfortable with how any information you provide may be used.
We think our customers understand better than anyone else how Red Hat can most effectively serve their needs. Because of this, Red Hat makes every effort to allow our customers to define the relationship they will have with us. We ask our customers how they would like Red Hat to communicate with them, if at all. We disclose how we will be using our customers' information through documents like this one, or by answering individual questions customers may ask. Also, we never sell our customers' information or provide it to others without making it clear that we intend to do so at the time the information is collected.
If you have any questions about any of these practices, please feel free to contact us at feedback@redhat.com.
Information Collected During Web Registration
Back
Next
Cancel

Figure 5.5. Red Hat Privacy Statement

5.3. Registering a User Account

Before you can create a System Profile, you must create a user account. The only required information in this section is a unique username, password, and a valid email address.

In the screen shown in Figure 5.7, “Create a Unique Username and Password”, you must choose a username and password. Once logged in to Red Hat Network, you can modify your preferences, view your existing System Profile, or obtain the latest Red Hat software packages. You must choose a unique username. If you enter one already in use, you will see an error message (see Figure 5.6, “Error: Username Already Exists”). Try different usernames until you find one that has not been used.

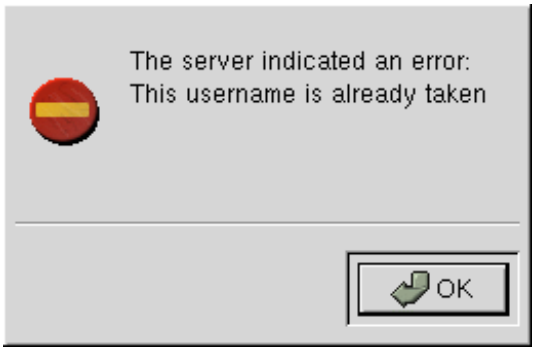


Figure 5.6. Error: Username Already Exists

Note

If you are already a member of redhat.com, you can use the same user name and password. However, you must continue with the registration process to create your System Profile.

Your username has the following restrictions:

- Cannot contain any spaces
- Cannot contain the characters & +, %, or '
- Is not case-sensitive, thereby eliminating the possibility of duplicate usernames differing only by capitalization

In addition, the following restrictions apply to both your username and password:

- Must be at least four characters long
- Cannot contain any tabs
- Cannot contain any line feeds

Passwords are case-sensitive for obvious reasons.

If you have already registered a machine and created a System Profile, you can add a new machine to your account. Run the **Red Hat Network Registration Client** on the new machine you wish to add, and enter your existing Red Hat Network username and password. The new machine is added to your existing account, and you can log into Red Hat Network with your username and password to view all your systems simultaneously.

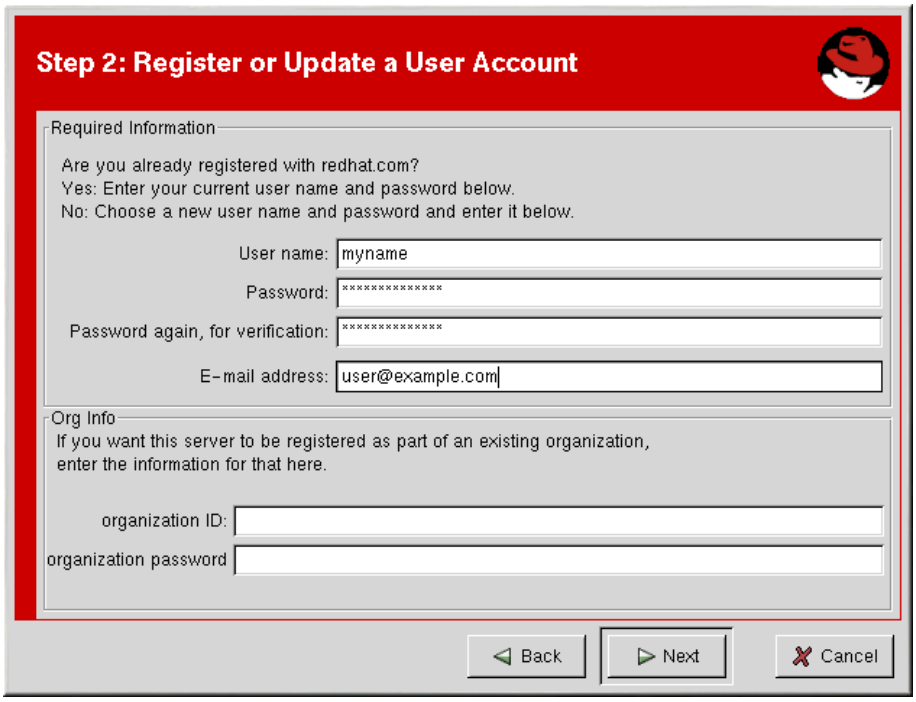

Step 2: Register or Update a User Account
Required Information
Are you already registered with redhat.com?
Yes: Enter your current user name and password below.
No: Choose a new user name and password and enter it below.
User name:
myname
Password:
Password again, for verification:
E-mail address:
user@example.com
Org Info
If you want this server to be registered as part of an existing organization,
enter the information for that here.
organization ID:
organization password
Back
Next
Cancel

Figure 5.7. Create a Unique Username and Password

Most users can leave the **Org Info** section blank. If you have an existing organization account, work with your Organization Administrator to ensure that your system is added to that account.This requires entering your organization's ID and password in the provided text fields. If the values are valid, the system is added to the organization's Red Hat Network account. Your Organization Administrator can then create your user account through the **Users** category of the RHN website. Refer to Section 6.8, "Users — " for instructions.

Click **Next** to continue.

5.4. Registering a System Profile

Now that you have a user account, you can create a System Profile that consists of hardware and software information about your Red Hat Enterprise Linux system. The software System Profile information is used by Red Hat Network to determine what software update notifications you receive.

5.4.1. Hardware System Profile

After creating a username and password for your Red Hat Network account, the **Red Hat Network Registration Client** probes your system for the following information:

- Red Hat Enterprise Linux version
- Hostname
- IP address
- CPU model
- CPU speed
- Amount of RAM
- PCI devices
- Disk sizes

- Mount points

The next step is choosing a profile name for your system as shown in Figure 5.8, “System Profile - Hardware”. The default value is the hostname for the system. You may modify this to be a more descriptive string, such as **`Email Server for Support Team`**. Optionally, you can enter a computer serial or identification number for the system.

If you do not wish to include information about your hardware or network in your System Profile, deselect **`Include information about hardware and network`** (see Figure 5.8, “System Profile - Hardware”).

Click **`Next`** to continue with the registration process.

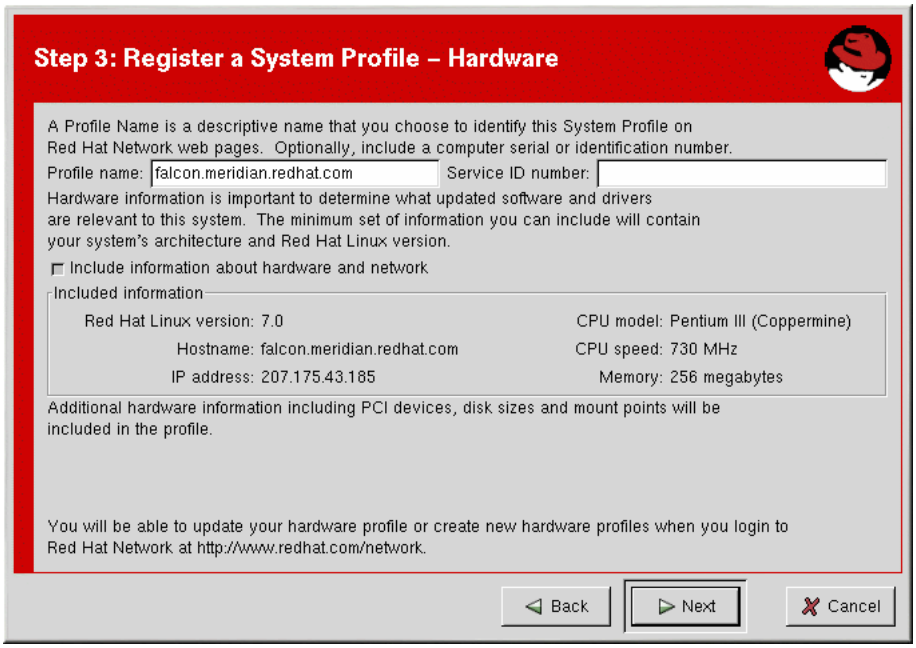

Step 3: Register a System Profile – Hardware
A Profile Name is a descriptive name that you choose to identify this System Profile on Red Hat Network web pages. Optionally, include a computer serial or identification number.
Profile name: falcon.meridian.redhat.com
Service ID number:
Hardware information is important to determine what updated software and drivers are relevant to this system. The minimum set of information you can include will contain your system's architecture and Red Hat Linux version.
Include information about hardware and network
Included information
Red Hat Linux version: 7.0
CPU model: Pentium III (Coppermine)
Hostname: falcon.meridian.redhat.com
CPU speed: 730 MHz
IP address: 207.175.43.185
Memory: 256 megabytes
Additional hardware information including PCI devices, disk sizes and mount points will be included in the profile.
You will be able to update your hardware profile or create new hardware profiles when you login to Red Hat Network at http://www.redhat.com/network.
Back
Next
Cancel

Figure 5.8. System Profile - Hardware

5.4.2. Software System Profile

The software System Profile consists of a list of RPM packages for which you wish to receive notifications. The **Red Hat Network Registration Client** displays a list of all RPM packages listed in the RPM database on your system and then allows you to customize the list by deselecting packages.

5.4.2.1. Gathering RPM Database Information

Only those packages you choose during this part of the registration are included in your System Profile, and you will only receive notifications about the packages in your System Profile. Thus, if you use an older version of a package and deselect it from the list, it will not be replaced with a newer version. This RPM list can be modified through the Red Hat Network website or by using the **Red Hat Update Agent**. Figure 5.9, “Registration Wizard” shows the progress bar displayed while the **Red Hat Network Registration Client** gathers a list of the RPM packages installed on your system. This operation may take some time depending on your system.

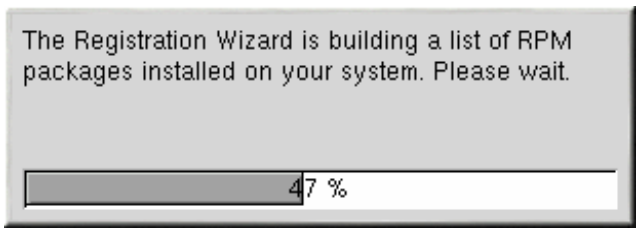


Figure 5.9. Registration Wizard

Once the RPM package list is built, the list is displayed as shown in Figure 5.10, "RPM Package Information". Deselecting **`Include RPM Packages installed on this system in my System Profile`** omits this information from your System Profile.

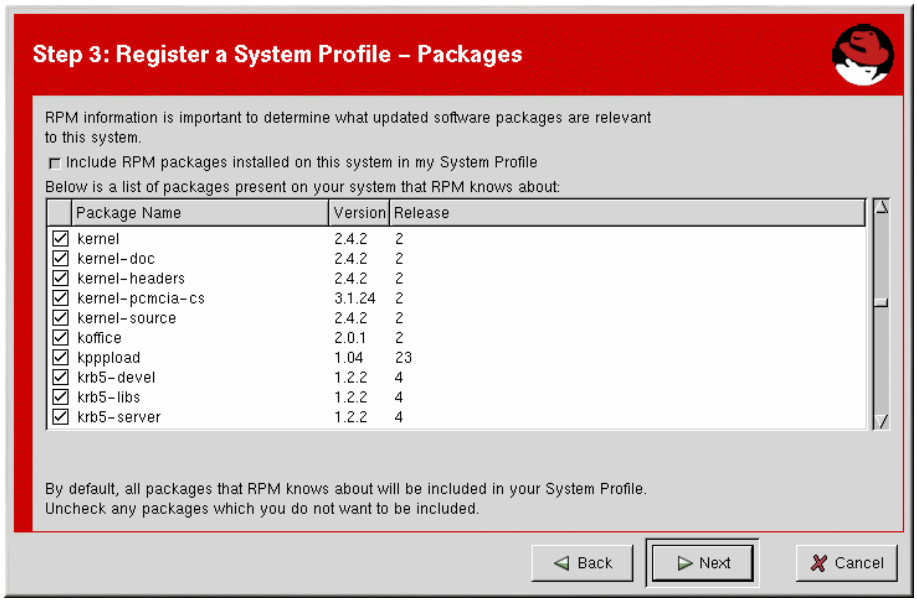

Step 3: Register a System Profile – Packages
RPM information is important to determine what updated software packages are relevant to this system.
Include RPM packages installed on this system in my System Profile
Below is a list of packages present on your system that RPM knows about:
Package Name Version Release
kernel 2.4.2 2
kernel-doc 2.4.2 2
kernel-headers 2.4.2 2
kernel-pcmcia-cs 3.1.24 2
kernel-source 2.4.2 2
koffice 2.0.1 2
kpppload 1.04 23
krb5-devel 1.2.2 4
krb5-libs 1.2.2 4
krb5-server 1.2.2 4
By default, all packages that RPM knows about will be included in your System Profile.
Uncheck any packages which you do not want to be included.
Back
Next
Cancel

Figure 5.10. RPM Package Information

5.4.2.2. Choosing RPM Packages to Exclude from the System Profile

By default, all RPM packages in your RPM database are included in your System Profile to be updated by Red Hat Network. To exclude a package, uncheck the package from the list by clicking the checkbox beside the package name. For example, Figure 5.11, "Choose which RPM Packages to Exclude from System Profile" shows that the **`procmail`**, **`procps`**, and **`psgml`** packages have been omitted from the package list.

Choose which packages to exclude, if any, from the System Profile, and click **`Next`** to continue with the registration process.

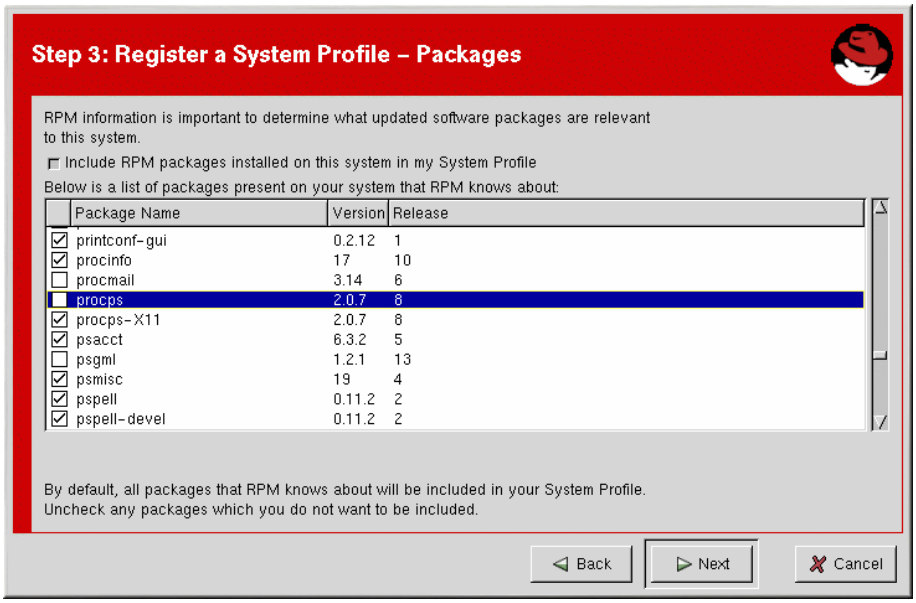

Step 3: Register a System Profile – Packages
RPM information is important to determine what updated software packages are relevant to this system.
Include RPM packages installed on this system in my System Profile
Below is a list of packages present on your system that RPM knows about:
Package Name
Version
Release
printconf-gui 0.2.12 1
procinfo 17 10
procmail 3.14 6
procps 2.0.7 8
procps-X11 2.0.7 8
psacct 6.3.2 5
psgml 1.2.1 13
psmisc 19 4
pspell 0.11.2 2
pspell-devel 0.11.2 2
By default, all packages that RPM knows about will be included in your System Profile.
Uncheck any packages which you do not want to be included.
Back
Next
Cancel

Figure 5.11. Choose which RPM Packages to Exclude from System Profile

5.5. Finishing Registration

As seen in Figure 5.12, “Finished Collecting Information for System Profile”, the last step of registration is to confirm that you want to send your System Profile to the Red Hat Network. If you choose **`Cancel`** at this point, no information is sent. Clicking **`Next`** submits your RHN System Profile.

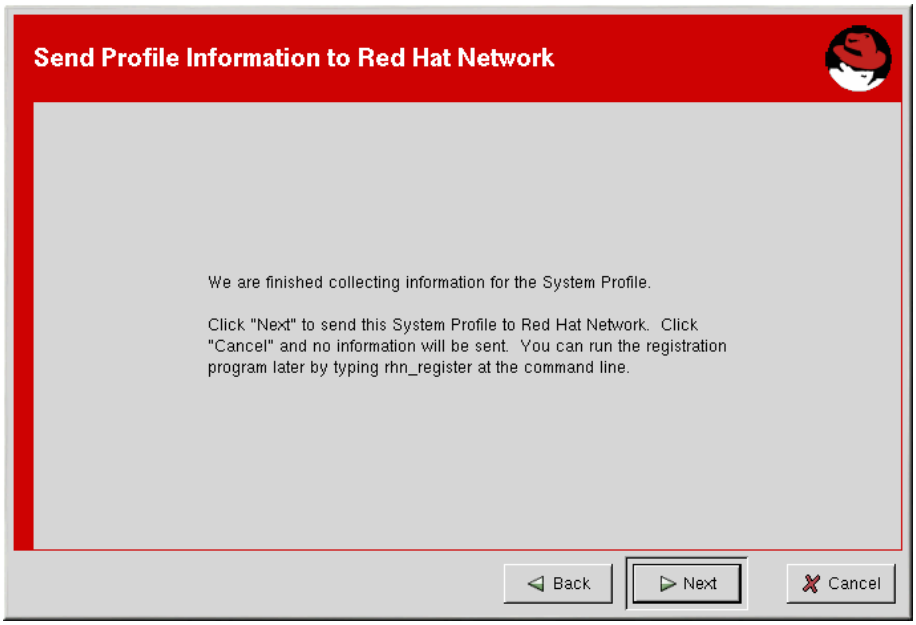

Send Profile Information to Red Hat Network
We are finished collecting information for the System Profile.
Click "Next" to send this System Profile to Red Hat Network. Click "Cancel" and no information will be sent. You can run the registration program later by typing rhn_register at the command line.
Back
Next
Cancel

Figure 5.12. Finished Collecting Information for System Profile

Figure 5.13, “Send System Profile to Red Hat Network” shows the progress bar displayed while your profile is sent. This process may take some time depending on your connection speed.

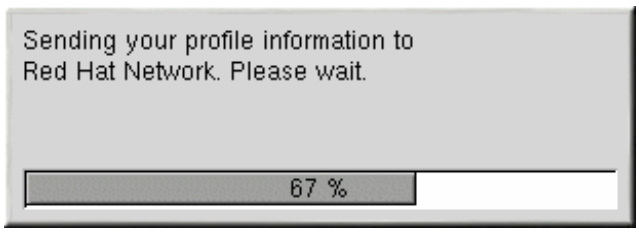


Figure 5.13. Send System Profile to Red Hat Network

The Red Hat Network Registration Client displays the **Registration Finished** screen (Figure 5.14, "Registration Finished" once your System Profile has been sent successfully. Click **Finish** to exit the **Red Hat Network Registration Client**.

After completing the registration, you must entitle your system to an RHN service level. Refer to Section 5.6, "Entitling Your System" for details.

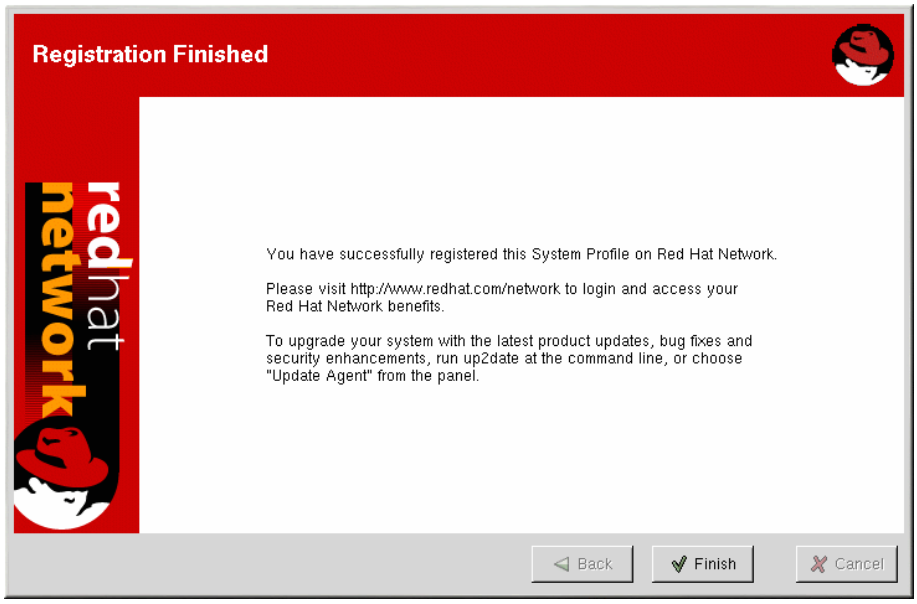

Registration Finished
redhat network
You have successfully registered this System Profile on Red Hat Network.
Please visit http://www.redhat.com/network to login and access your Red Hat Network benefits.
To upgrade your system with the latest product updates, bug fixes and security enhancements, run up2date at the command line, or choose "Update Agent" from the panel.
Back
Finish
Cancel

Figure 5.14. Registration Finished

5.6. Entitling Your System

Now that you have registered your system, it must be entitled before you can receive updated packages. In other words, you must subscribe it to a service level offering.

To entitle a system, go to http://rhn.redhat.com and log in using the same username and password you just used in the **Red Hat Network Registration Client**. Click **Systems** on the top navigation bar and then **Systems Entitlements** in the left navigation bar.

The **System Entitlements** page displays the following items:

- a list of the system for which the user can choose an entitlement level
- the current entitlements applied to each of these systems
- buttons that allow the user to change entitlement level
- an overview of the number and types of purchased entitlements that remain available to the

organization

To change the entitlement level of a system or systems, check the box to the left of the systems and click the appropriate button for the desired entitlement level. Note that you must apply a Management entitlement to a system before you can add a Provisioning entitlement. You can change entitlements to any available level at any time.

Note

Removing a required entitlement (such as Provisioning) will not cancel a previously scheduled action (such as a kickstart).

As you change the selected entitlements for your systems, the number of available entitlements is updated at the bottom of the screen.

5.7. Text Mode RHN Registration Client

If you are not running the X Window System, the **Red Hat Network Registration Client** starts in text mode.

You can force the **Red Hat Network Registration Client** to run in text mode with the command:

```
rhn_register --nox
```

The screens for the text mode **Red Hat Network Registration Client** are almost identical to the screens for the graphical **Red Hat Network Registration Client**. Some of the text in the text mode version is more concise due to lack of space in the interface. However, there are equal numbers of screens and fields in both versions. Thus, if you are using the text mode version, you can still follow the instructions that begin in Section 5.2, “Starting the **Red Hat Network Registration Client**”.

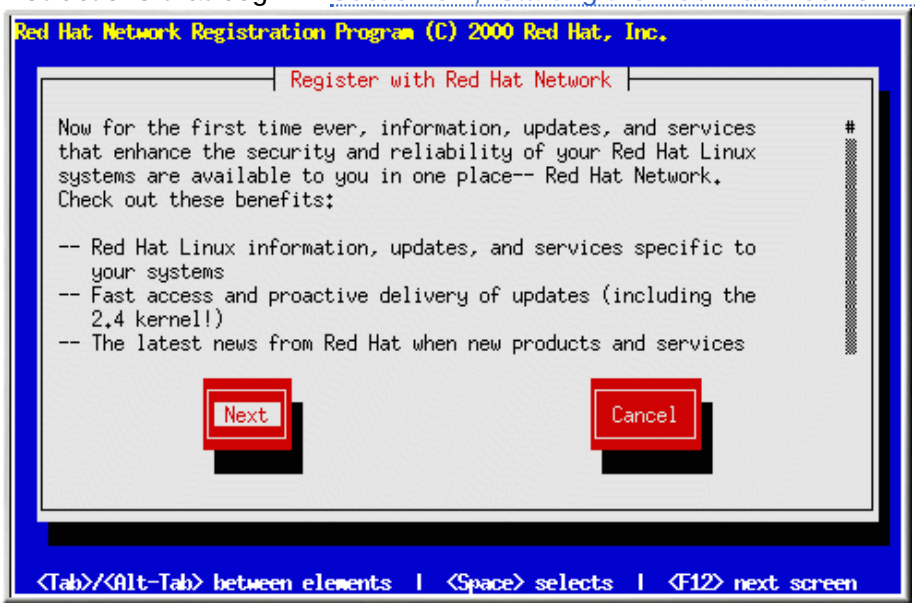

Red Hat Network Registration Program (C) 2000 Red Hat, Inc.
Register with Red Hat Network
Now for the first time ever, information, updates, and services
that enhance the security and reliability of your Red Hat Linux
systems are available to you in one place-- Red Hat Network.
Check out these benefits:
-- Red Hat Linux information, updates, and services specific to
your systems
-- Fast access and proactive delivery of updates (including the
2.4 kernel!)
-- The latest news from Red Hat when new products and services
Next
Cancel
<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Figure 5.15. Text Mode Welcome Screen

Chapter 6. Red Hat Network Website

You can use the Red Hat Network website to manage multiple Red Hat Enterprise Linux systems simultaneously, including viewing Errata Alerts, applying Errata Updates, and installing packages. This chapter seeks to identify all of categories, pages, and tabs within the website and explain how to use them.

6.1. Navigation

The **Top Navigation Bar** is divided into tabs. Organization Administrators see the following **Top Navigation Bar**. Note that only RHN Satellite customers see the Monitoring and **Satellite Tools** tabs.

Figure 6.1. Top Navigation bar — RHN Satellite

Figure 6.2. Top Navigation bar — RHN's Hosted Environment

The **Left Navigation Bar** is divided into pages. The links are context-sensitive and may vary slightly between RHN Satellite and non-Satellite web interfaces. The following is an exaple of the **Left Navigation Bar** for the **Users** tab.

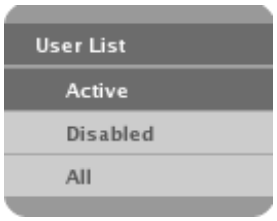


Figure 6.3. Left Navigation Bar — Users

Some pages have sub-tabs. These tabs offer an additional layer of granularity in performing tasks for systems or users. The following is a menu bar for all System Details sub-tabs. This system has Management and Provisioning entitlements, but not Monitoring:

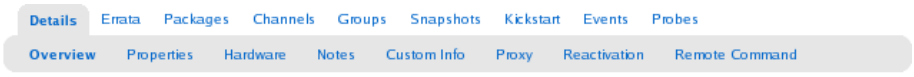


Figure 6.4. Sub-Tabs — System Details

6.1.1. Entitlement Views

Keep in mind, since this guide covers all entitlement levels, some tabs, pages, and even whole categories described here may not be visible to you. For this reason, icons are used here to identify which functions are available to each entitlement level.

Table 6.1. Entitlement Icons

Icon	Entitlement
	Management or higher
	Provisioning
	Monitoring

If no icon follows a category, page, or tab label within this chapter, the area described is available to all Red Hat Network users. If an icon does follow, the associated entitlement is needed. Remember that Provisioning inherits all of the functions of Management.

If an icon precedes a paragraph, only the specific portion of the page or tab discussed afterward requires the indicated entitlement level. When a page or tab is associated with a particular entitlement level, all of its tabs and subtabs require at least the same entitlement level but may need a higher entitlement. Regardless, each tab is identified separately.

6.1.2. Categories and Pages

This section summarizes all of the categories and primary pages (those linked from the top and left navigation bars) within the RHN website. It does not list the many subpages, tabs and subtabs accessible from the left navigation bar and individual pages. Each area of the website is explained in detail later in this chapter:

- **`Your RHN`** — View and manage your primary account information and obtain help.
  - **`Your RHN`** — Obtain a quick overview of your account. It notifies you if your systems need attention, provides a quick link to go directly to them, and displays the most recent Errata Alerts for your account.
  - **`Your Account`** — Update your personal profile and addresses.
  - **`Your Preferences`** — Indicate if you wish to receive email notifications about Errata Alerts for your systems, set how many items are displayed at one time for lists such as system lists and system group lists, set your time zone, and identify your contact options.
  - **`Purchase History`** — View a history of your entitlements, including the expiration date and the number available.
  - **`Help`** — Learn how to use Red Hat Network and receive support if needed.
- **`Systems`** — Manage your systems here.
  - **`Overview`** — — View a summary of your systems or system groups showing how many Errata Alerts each system has and which systems are entitled.
  - **`Systems`** — Select and view subsets of your systems by specific criteria, such as Out of Date, Unentitled, Ungrouped, and Inactive.
  - **`System Groups`** — — List your system groups. Create additional groups.
  - **`System Set Manager`** — — Perform actions on currently selected systems.
  - **`System Entitlements`** — Change the entitlement levels of systems.
  - **`Advanced Search`** — — Quickly search all of your systems by specific criteria, such as name, hardware, devices, system info, networking, packages, and location.
  - **`Activation Keys`** — — Generate an activation key for an RHN-entitled system. This activation key can be used to grant a specified level of entitlement or group membership to a

newly registered system with the **rhnreg_ks** command.

- **Stored Profiles** — — View system profiles used to provision systems.
- **Custom System Info** — — Create and edit system information keys containing completely customizable values that can be assigned while provisioning systems.
- **Kickstart** — — Display and modify various aspects of kickstart profiles used in provisioning systems.

- **Errata** — View and manage Errata Alerts here.
  - **Errata** — List Errata Alerts and download associated RPMs.
  - **Advanced Search** — Search Errata Alerts based on specific criteria, such as synopsis, advisory type, and package name.
- **Channels** — View and manage the available RHN channels and the files they contain.
  - **Software Channels** — View a list of all software channels and those applicable to your systems.
  - **Channel Entitlements** — View a list of software channels for which you have paid, as well as the systems associated with each.
  - **Download Software** — Access priority downloading of Red Hat ISO images. ISO images are used to write to CD.
  - **Package Search** — Search packages using all or some portion of the package name.
  - **Manage Config Channels** — — Create and edit channels used to deploy configuration files.
- **Schedule** — Keep track of your scheduled actions.
  - **Pending Actions** — List scheduled actions that have not been completed.
  - **Failed Actions** — List scheduled actions that have failed.
  - **Completed Actions** — List scheduled actions that have been completed. Completed actions can be archived at any time.
  - **Archived Actions** — List completed actions that have been selected to archive.
- **Users** — — View and manage users for your organization.
  - **User List** — — List users for your organization.
- **Monitoring** — — Run probes and receive notifications regarding systems.
  - **Probe Status** — — View probes by state.
  - **Notification** — — View contact methods established for your organization.
  - **Scout Config Push** — — Reconfigure your monitoring infrastructure.
  - **Global Config** — — Change organization-wide monitoring settings.

6.1.3. Errata Alert Icons

Throughout Red Hat Network you will see three Errata Alert icons. represents a Security Alert. represents a Bug Fix Alert. represents an Enhancement Alert.

In the **Your RHN** page, click on the Errata advisory to view details about the Erratum or click on the number of affected systems to see which are affected by the Errata Alert. Both links take you to tabs of the **Errata Details** page. Refer to Section 6.5.2.2, “Errata Details” for more information.

6.1.4. Quick Search

In addition to the Advanced Search functionality offered within some categories, the RHN website also offers a Quick Search tool near the top of each page. To use it, select the item type (such as packages) and type a keyword to look for a name match. Click the **Search** button. Your results appear at the bottom of the page. Refer to the appropriate category for instructions on using these results.

6.1.5. Systems Selected

Also near the top of the page is a tool for keeping track of the systems you have selected for use in the System Set Manager. It identifies the number of selected systems at all times and provides the means to work with them. Clicking the **Clear** button deselects all systems, while clicking the **Manage** button launches the System Set Manager with your selected systems in place.

These systems can be selected in a number of ways. Only systems with at least a Management entitlement are eligible for selection. On all system and system group lists, a Select column exists for this purpose. Select the checkboxes next to the systems or groups and click the **Update List** button below the column. Each time, the Systems Selected tool at the top of the page changes to reflect the new number of systems ready for use in the System Set Manager. Refer to Section 6.4.4, “System Set Manager — ” for details.

6.1.6. Lists

The information within most categories is presented as lists. These lists have some common features for navigation. For instance, you can navigate through virtually all lists by clicking the back and next arrows above and below the right side of the table. Some lists also offer the ability to retrieve items alphabetically by clicking the letters above the table.

6.2. Logging into the RHN Website

Use a web browser to navigate to http://rhn.redhat.com. RHN displays the login page shown below unless one of two things is true:

- You have recently logged into your account at http://www.redhat.com.
- You have recently either logged into RHN or recently visited the new account verification page.

If you have recently logged into http://rhn.redhat.com or http://www.redhat.com, you are automatically authenticated and redirected to the **Your RHN** page.

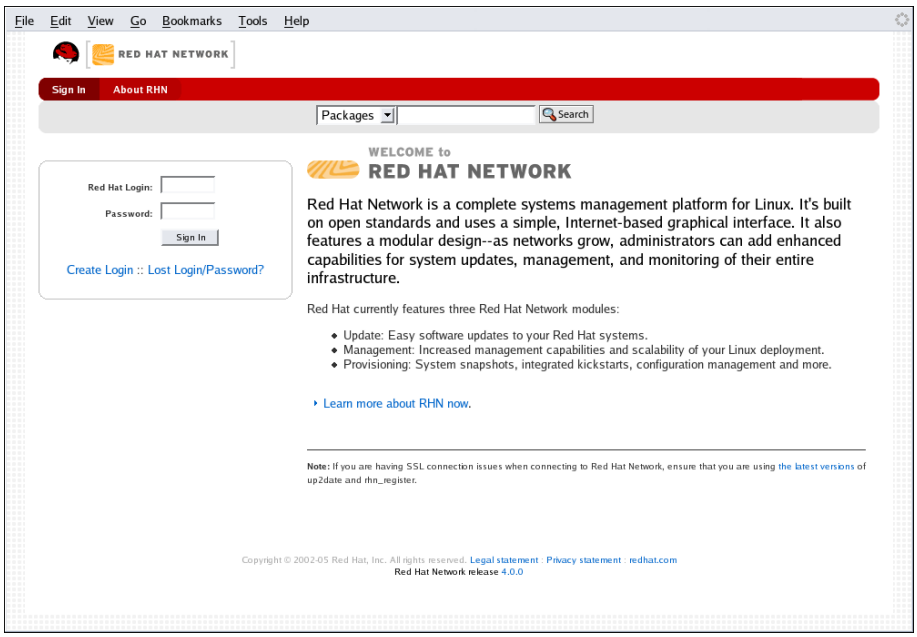

File Edit View Go Bookmarks Tools Help
RED HAT NETWORK
Sign In
About RHN
Packages
Search
Red Hat Login:
Password:
Sign In
Create Login :: Lost Login/Password?
WELCOME to
RED HAT NETWORK
Red Hat Network is a complete systems management platform for Linux. It's built on open standards and uses a simple, Internet-based graphical interface. It also features a modular design--as networks grow, administrators can add enhanced capabilities for system updates, management, and monitoring of their entire infrastructure.
Red Hat currently features three Red Hat Network modules:
Update: Easy software updates to your Red Hat systems.
Management: Increased management capabilities and scalability of your Linux deployment.
Provisioning: System snapshots, integrated kickstarts, configuration management and more.
Learn more about RHN now.
Note: If you are having SSL connection issues when connecting to Red Hat Network, ensure that you are using the latest versions of up2date and rhn_register.
Copyright © 2002-05 Red Hat, Inc. All rights reserved. Legal statement : Privacy statement : redhat.com
Red Hat Network release 4.0.0

Figure 6.5. RHN Website

If you have not registered a system yet or do not have a redhat.com account, create a new account by following the **Learn More** link, then selecting **Create Login** on the resulting page. After creating a new user account, you must register a system before using RHN. Refer to Chapter 2, ***Red Hat Update Agent*** for step-by-step instructions.

After registering your system with Red Hat Network, go back to http://rhn.redhat.com and complete the username and password fields with the same information established during registration. Once complete, press the **Log In** button to continue.

Tip

You may click the **Sign In** tab at the top of the screen to display the fields if they are not already visible.

If you have not previously accepted the **RHN Site Terms** and the **T7** agreement, you will be asked to do so now before proceeding. To read the content of either agreement, click on its title, which will open a new window. When ready to proceed, select the checkbox indicating your acceptance of the agreements and press the **Continue** button.

Note

You must accept both the Site Terms and the T7 agreement in order to use RHN.

Once you have accepted the agreements and pressed the **Continue** button, RHN displays the **Your RHN** page.

6.3. Your RHN

After logging into the website of Red Hat Network, the first page to appear is **Your RHN**. This page contains important information about your systems, including summaries of system status, actions, and Errata Alerts.

Tip

If you are new to the RHN website, it is recommended that you read Section 6.1, “Navigation” to become familiar with the layout and symbols used throughout the website.

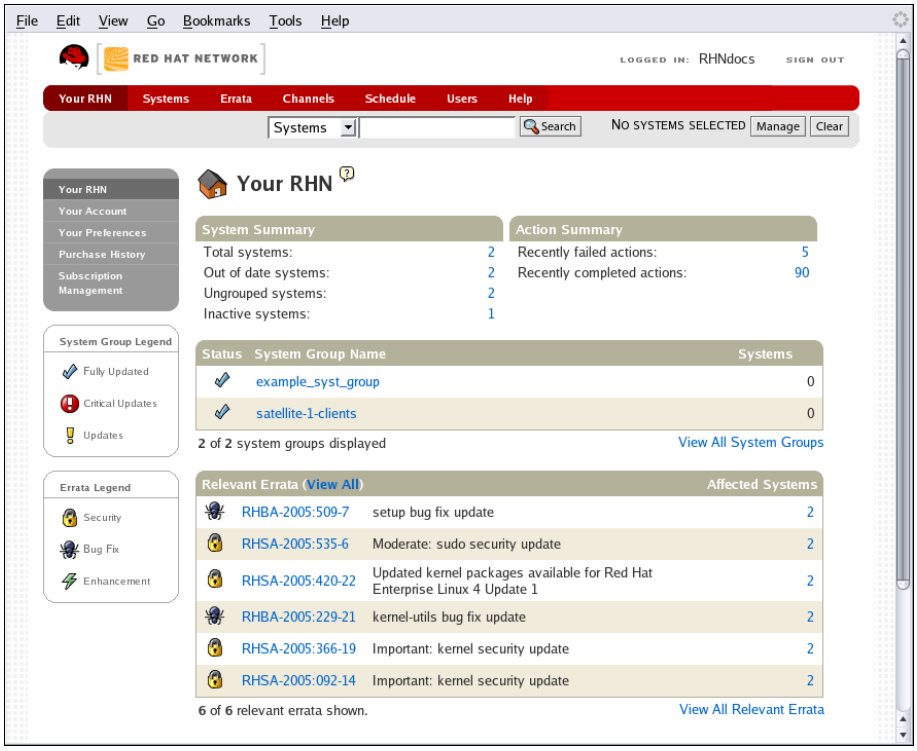


Figure 6.6. Your Red Hat Network

This page is broken into functional areas, with the most critical areas displayed first. Users can control which of the following areas are displayed by making selections on the **Your RHN** ⇒ **Your Preferences** page. Refer to Section 6.3.2, “Your Preferences” for more information.

- The **Tasks** area lists the most common tasks that an administrator performs via the web. Click on any of the links to be taken to the page within RHN that allows you to accomplish that task.
- To the right is the **Inactive System** listing. If any systems have not been checking in to RHN, they are listed here. Highlighting them in this way allows an administrator quickly select those systems for troubleshooting.
- — Customers with Monitoring enabled on their Satellite can also choose to include a list of all probes in the Warning state.
- — Customers with Monitoring enabled on their Satellite can also choose to include a list of all probes in the Critical state.
- The section below lists the most critical systems within your organization. It provides a link to quickly view those systems, and displays a summary of the errata updates that have yet to be applied to those systems. Click on the name of the system to be taken to the **System Details** page of that

system and apply the errata updates. Below the list is a link to the **Out of Date** systems page.

- Next is the **Recently Scheduled Actions** section. Any action that is less than thirty days old is considered to be recent. This section allows you to see all actions and their status, whether they have failed, completed, or are still pending. Click on the label of any given actions to view the details page for that action. Below the list is a link to the **Pending Actions** page, which lists all actions that have not yet been picked up by your client systems.
- The following section lists the Security Errata that are available and have yet to be applied to some or all of your client systems. It is critical that you apply these security errata to keep your systems secure. Below this section are links to all errata and to those errata that apply to your systems.
- The final section lists your **System Groups** and indicates whether the systems in those groups are fully updated. Click on the link below this section to be taken to the **System Groups** page, from which you can chose **System Groups** to use with the System Set Manager.

You can return to this page by clicking **Your RHN** on the left navigation bar.

6.3.1. Your Account

The **Your Account** page allows you to modify your personal information, such as name, password, and title. To modify any of this information, make the changes in the appropriate text fields and click the **Update** button in the bottom right-hand corner.

Remember, if you change your Red Hat Network password (the one used to log into RHN and redhat.com), you will not see your new one as you type it for security reasons. Also for security, your password is represented by 12 asterisks no matter how many characters it actually contains. Replace the asterisks in the **Password** and **Password Confirmation** text fields with your new password.

6.3.1.1. Addresses

The **Addresses** page allows you to manage your mailing, billing and shipping addresses, as well as the associated phone numbers. Just click **Edit this address** below the address to be modified, make the changes, and click **Update Address**.

6.3.1.2. Change Email

The email address listed in the **Your Account** page is the address to which Red Hat Network sends email notifications if you select to receive Errata Alerts or daily summaries for your systems on the **Your Preferences** page.

To change your preferred email address, click **Change Email** in the left navigation bar. You are then asked for the new email address. Enter it and click the **Update** button. A confirmation email is sent to the new email address; responding to the confirmation email validates the new email address. Note that false email addresses such as those ending in "@localhost" are filtered and rejected.

6.3.1.3. Account Deactivation

The **Account Deactivation** page provides a means to cancel your Red Hat Network service. Click the **Deactivate Account** button to deactivate your account. The web interface returns you to the login screen. If you attempt to log back in, an error message advises you to contact the Organization Administrator for your organization. Note that if you are the only Organization Administrator for your organization, you are unable to deactivate your account.

6.3.2. Your Preferences

The **Your Preferences** page allows you to configure Red Hat Network options, including:

- Email Notifications — Determine whether you want to receive email every time an Errata Alert is applicable to one or more systems in your RHN account.

Important

This setting also enables Management and Provisioning customers to receive a daily summary of system events. These include actions affecting packages, such as scheduled Errata Updates, system reboots, or failures to check in. In addition to selecting this checkbox, you must identify each system to be included in this summary email. (By default, all Management and Provisioning systems are included in the summary.) This can be done either individually through the **System Details** page or for multiple systems at once through the **System Set Manager** interface. Note that RHN sends these summaries only to verified email addresses. To disable all messages, simply deselect this checkbox.

- RHN List Page Size — Maximum number of items that appear in a list on a single page. If more items are in the list, clicking the **Next** button displays the next group of items. This preference applies to system lists, Errata lists, package lists, and so on.
- "Your RHN" Start Page — select the information areas that are displayed on the **Your RHN** Start Page. Check the box to the left of the information area you would like to include.

After making changes to any of these options, click the **Save Preferences** button in the bottom right-hand corner.

6.3.3. Locale Preferences

The **Your RHN** ⇒ **Locale Preferences** page allows each user to tailor their RHN interface to the local time and their preferred language. Select the appropriate timezone from the **Time Zone** dropdown box, then click the **Save Preferences** button to apply the selection.

When the language preference is set to **Use Browser Settings**, RHN uses the language preference from the user's browser (such as **Firefox**) to determine which language to use for the web interface. When one of the listed languages is selected, the user sees the web interface in that language each time they log in, regardless of their browser's settings. Choosing a preferred language may be helpful for users traveling abroad. To select a default language, click the radio button to the left of the appropriate language and click the **Save Preferences** button to apply the change.

6.3.4. Subscription Management

To use all of the features of RHN, your systems must be *entitled* — subscribed to an RHN service level. Use the **System Entitlements** page to configure which systems are entitled to which service offerings. There are four primary types of entitlements:

- **Update** — manages a single Red Hat Enterprise Linux system. It includes Errata Alerts, Scheduled Errata Updates, Package Installation, and the **Red Hat Update Agent**.
- **Management** — manages multiple systems with multiple system administrators. In addition to the features of the Update offering, it includes system group management, user management, and the **System Set Manager** interface to quickly perform actions on multiple systems.
- **Provisioning** — offers the highest level of functionality. It should be used to provision multiple systems that will need to be re-installed and reconfigured regularly. The Provisioning offering provides tools for kickstarting machines, managing their configuration files, conducting snapshot rollbacks, and inputting searchable custom system information, as well as all of the functionality

included in the Management service level.

- **Monitoring** — monitors the health of multiple systems. The Monitoring offering provides probes that watch system metrics and notify Administrators when changes occur. Such notifications alert Administrators to system performance degradation before it becomes critical.
- **Virtualization** — applies to virtual host systems. Virtual hosts with this entitlement may register as many as four guest systems without violating RHN's Service Level Agreement. Guest systems may be subscribed to any channel with the **virtualization-free** channel group label without consuming channel entitlements. Subscribing a guest to any channel that does not belong to **virtualization-free**, such as a Directory Server or RHN Satellite channel, consumes an additional channel entitlement.
- **Virtualization Platform** — also applies to virtual host systems. Host systems to which this entitlement apply may register an unlimited number of virtual guests without invalidating your Service Level Agreement. Guests of a host with this entitlement may subscribe to any channel that has the **virtualization-platform-free** content group label without consuming any channel entitlements. Subscribing a guest to any channel that does not belong to **virtualization-platform-free**, such as a Directory Server or RHN Satellite channel, consumes an additional channel entitlement.

Tip

The two virtualization entitlements specifically apply to host systems.
Guest systems that exist on unregistered hosts are treated the same as any physical system — each guest consumes a channel and a system entitlement.

6.3.4.1. System Entitlements

The **System Entitlements** page allows you to view, add, and remove the entitlements for your registered systems. Red Hat Network 4.0 allows you to apply and remove entitlements at will, allowing you to adjust your Red Hat Network infrastructure as your organization grows and changes.

To change an individual base entitlement, select the checkbox to the left of the system, then click the button that corresponds to the entitlement you wish to add. For add-on entitlements, select the system's checkbox, followed by the desired entitlement from the drop-down box, and finally press the **Add Entitlement** button.

If clicking on an entitlement fails to update the information in the table, you may need to purchase additional entitlements. Check the number of available subscriptions, listed in bold below the table. Non-RHN Satellite customers may purchase more entitlements; click the **Buy Now** link at the left of the page to do so.

When an entitlement expires, the last system entitled to the same service level (such as Management) will be unentitled. For instance, if you have 10 Red Hat Enterprise Linux AS systems entitled to Management and either one of the RHN entitlements or one of the operating system subscriptions expire, the last system subscribed or entitled will have their subscription or entitlement removed.

6.3.4.2. Virtualization Entitlements

This page only appears if you have applied Virtualization or Virtualization Platform entitlements. It allows you to quickly assess whether you have used these entitlements in the most effective manner.

The first table on this page displays any Virtualization-entitled hosts that have more guest systems than are allowed in the Red Hat Network service level agreement. If you would like to upgrade these systems

to any available Virtualization Platform entitlements, click the profile name of that system. This displays the **System Details** page for the system. Click the **Edit Properties** link on the page to edit that system's add-on entitlements.

The second table displays any Virtualization Platform-entitled hosts that have fewer than four guests. It may be advisable to to downgrade these systems' entitlements to the Virtualization entitlement. To do so, click the profile name of the system you would like to downgrade, then edit the add-on entitlements from the resulting **System Details** page.

6.3.4.3. Software Channel Entitlements

The software channels listed on this page are the subscription-based channels to which your organization has paid access. The table lists each of the supported operating systems that can be managed via RHN, the number of such systems you have registered with RHN, and finally the remaining number of entitlements for that operating system. Clicking on the name of the channel opens a page that displays information about the channels associated with that channel entitlement. Clicking on the number of entitled systems displays a list of the systems so entitled.

6.3.4.4. Purchase or Renew

This page is only visible to RHN Hosted customers.

As the title suggests, this page provides links to the main Red Hat site, from which you can renew or purchase entitlements. The **Red Hat Renewal Center** can renew both your Red Hat Enterprise Linux subscription and your Red Hat Network entitlements. The **Red Hat Store** can provide additional entitlements.

6.3.4.5. Expiration Dates &Purchase History

The **Purchase History** page provides a link to the main Red Hat site, where you can view your purchase history and the expiration dates for web and phone support, Red Hat Enterprise Linux subscriptions, and Red Hat Network software and service entitlements.

6.4. Systems

If you click the **Systems** tab on the top navigation bar, the **Systems** category and links appear. The pages in the **Systems** category allow you to select systems so that you can perform actions on them and create System Profiles.

6.4.1. Overview —

The **Overview** page provides a summary of your systems, including their status, number of associated Errata and packages, and entitlement level. Clicking on the name of a system takes you to its **System Details** page. Refer to Section 6.4.2.9, “System Details” for more information.

Clicking the **View System Groups** link at the top of the **Overview** page takes you to a similar summary of your system groups. It identifies group status and displays the number of systems contained. Clicking on the number of systems takes you to the **Systems** tab of the **System Group Details** page, while clicking on the system name takes you to the **Details** tab for that system. Refer to Section 6.4.3.3, “System Group Details — ” for more information.

You can also click the **Use Group** button in the **System Groups** section of the **Overview** page to go directly to the **System Set Manager**. Refer to Section 6.4.4, “System Set Manager — ” for more

information.

6.4.2. Systems

The **Systems** page displays a list of all of your registered systems. The **Systems** list contains several columns of information for each system:

- **Select** — Update or unentitled systems cannot be selected. To select systems, mark the appropriate checkboxes. Selected systems are added to the **System Set Manager**. After adding systems to the **System Set Manager**, you can use it to perform actions on them simultaneously. Refer to Section 6.4.4, “System Set Manager — ” for details.
- **Status** — Shows which type of Errata Alerts are applicable to the system or confirms that it is up-to-date. Some icons are linked to pages providing resolution. For instance, the standard Updates icon is linked to the **Upgrade** subtab of the packages list, while the Critical Updates icon links directly to the **Update Confirmation** page. Also, the Not Checking In icon is linked to instructions for resolving the issue.
  - — System is up-to-date
  - — Critical Errata available, update *strongly* recommended
  - — Updates available and recommended
  - — System is locked; Actions prohibited
  - — System is being kickstarted
  - — Updates have been scheduled
  - — System not checking in properly (for 24 hours or more)
  - — System not entitled to any update service
- **Errata** — Total number of Errata Alerts applicable to the system.
- **Packages** — Total number of package updates for the system. Includes packages from Errata Alerts as well as newer packages that are not from Errata Alerts. For example, imagine a client system that has an early version of a package installed. If this client is then subscribed to the appropriate base channel of RHN (such as Red Hat Enterprise Linux 4), that channel may have an updated version of the package. If so, the package appears in the list of available package updates.

  Important

  If the RHN website identifies package updates for the system, yet the **Red Hat Update Agent** responds with "Your system is fully updated" when run, a conflict likely exists in the system's package profile or in the **up2date** configuration file. To resolve the conflict, either schedule a package list update or remove the packages from the Package Exceptions list for the **Red Hat Update Agent**. Refer to Section 6.4.2.9, “System Details” or Section 2.4.1.3, “Package Exceptions Settings”, respectively, for instructions.

- **System** — The name of the system as configured when registering it. The default name is the hostname of the system. Clicking on the name of a system takes you to the **System Details** page for the system. Refer to Section 6.4.2.9, “System Details” for more information.
- **Base Channel** — The primary channel for the system, based upon its operating system distribution. Refer to Section 6.6.1, “Software Channels” for more information.

- **Entitlement** — Whether or not the system is entitled and at what service level.

Links in the left navigation bar below **Systems** enable you to select and view predefined sets of your systems. All of the options described above can be applied within these pages.

6.4.2.1. All

The **All** page contains the default set of your systems. It displays every system you have permission to manage. A user has permission to manage a system if he is the only user in his organization, if he is an Organization Administrator, or if the system is a member of a group to which he has admin rights.

6.4.2.2. Virtual Systems

To reach this page, select the **Systems** tab, followed by the **Systems** subtab from the left navigation bar, and finally select **Virtual Systems** from the left navigation bar. This page lists each virtual host of which the RHN Satellite is aware and the guest systems on those hosts.

System

This column displays the name of each guest system.

Updates

This column indicates whether the guest systems have any errata that have not yet been applied to them.

Status

This column indicates whether a guest is running, paused, or stopped.

Base Channel

This column indicates the base channel to which the guest is currently subscribed.

Only those guests that are registered with RHN are displayed in blue text. Clicking on the hostname of such a guest system displays that system's **System Details** page.

6.4.2.3. Out of Date

The **Out of Date** page displays the systems that have applicable Errata Alerts that have not been applied.

6.4.2.4. Unentitled —

The **Unentitled** page displays the systems that have not yet been entitled for Red Hat Network service.

6.4.2.5. Ungrouped

The **Ungrouped** page displays the systems that have not yet been assigned to a specific system group.

6.4.2.6. Inactive

The **Inactive** page displays the systems that have not checked into RHN for 24 hours or more. When the **Red Hat Update Agent** connects to RHN to see if there are any updates available or if any actions

have been scheduled, this is considered a checkin. If you are seeing a message indicating checkins are not taking place, the RHN client on your system is not successfully reaching Red Hat Network for some reason. This indicates:

- The system is not entitled to any RHN service. System Profiles that remain unentitled for 180 days (6 months) are removed.
- The system is entitled, but the Red Hat Network Daemon has been disabled on the system. Refer to Chapter 3, *Red Hat Network Daemon* for instructions on restarting and troubleshooting.
- The system is behind a firewall that does not allow connections over https (port 443).
- The system is behind an HTTP proxy server that has not been properly configured.
- The system is connected to an RHN Proxy Server or RHN Satellite that has not been properly configured.
- The system itself has not been properly configured, perhaps pointing at the wrong RHN Server.
- The system is not on the network.
- Some other barrier exists between the system and the RHN Servers.

6.4.2.7. Satellite

The **`Satellite`** page displays the RHN Satellite systems registered to your RHN account.

6.4.2.8. Proxy

The **`Proxy`** page displays the RHN Proxy Server systems registered to your RHN account.

6.4.2.9. System Details

Click on the name of a system on any page and RHN displays the **`System Details`** page for that client. From here, you may modify the displayed information or remove the system altogether by clicking the **`delete system`** link on the top-right corner.

Note

The **`delete system`** link in the upper right of this screen refers to the system profile only. Deleting a host system profile will not destroy or remove the registration of guest systems. Deleting a guest system profile does not remove it from the list of guests for its host, nor does it stop or pause the guest. It does, however, remove your ability to manage it via RHN.
If you mistakenly delete a system profile from RHN, you may re-register the system.

The **`System Details`** page is further divided into the following tabs:

- Details
- Software
- Configuration
- Provisioning —
- Monitoring —
- Groups
- Events

The following sections discuss these tabs and their sub-tabs in detail.

6.4.2.9.1. System Details ⇒ Details

This page is not accessible from any of the standard navigation bars. However, clicking on the name of a system anywhere in the web interface brings you to this page. The default tab displayed on this page is the **Details** ⇒ **Overview** subtab. Other tabs are available, depending on the current entitlement level of the system.

6.4.2.9.1.1. System Details ⇒ Details ⇒ Overview

This system summary page displays the system status message and the following key information about the system:

System Info

System Status Message

This message indicates the current state of your system in relation to RHN.

Note

If updates are available for any entitled system, the message **Critical updates available** appears. To apply these updates, click the **update now** link.

system ID

A unique identifier generated each time a system registers with RHN.

Note

The system ID can be used to eliminate duplicate profiles from RHN. Compare the system ID listed on this page with the information stored on the client system in the **/etc/sysconfig/rhn/systemid** file. In that file, the system's current ID is listed under "system_id". The value starts after the characters "ID-" If the value stored in the file does not match the value listed in the profile, the profile is not the most recent one and may be removed.

Hostname

The hostname as defined by the client system. This information is often found in **/etc/hostname** for Red Hat Enterprise Linux systems.

IP Address

The IP address of the client.

Kernel

The kernel that is installed and operating on the client system.

Registered

The date and time at which the system registered with RHN and created this profile.

Checked In

The date and time at which the system last checked in with RHN.

Last Booted

The date and time at which the system was last started or restarted.

Note

Systems with a Management entitlement can be rebooted from this screen.

- Select **`Schedule system reboot`**
- Provide the earliest date and time at which the reboot may take place.
- Click the **`Schedule Reboot`** button in the lower right.

When the client checks in after the scheduled start time, RHN will instruct the system to restart itself.

Locked

Indicates whether a system has been locked.

Actions cannot be scheduled for locked systems through the web interface until the lock is removed manually. This does not include preventing auto-errata updates scheduled through the web interface. To prevent the application of auto-errata updates, de-select **`Auto Errata Update`** from the **`System Details`** ⇒ **`Details`** ⇒ **`Properties`** subtab.

Locking a system can help to prevent you from accidentally making any changes to a system until you are ready to do so. For example, the system may be a production system that you do not wish to receive updates or new packages until you decide to unlock it.

Important

Locking a system in the web interface *will not* prevent any actions that originate from the client system. For example, if a user logs into the client directly and runs **`up2date`**, **`up2date`** will install available errata whether or not the system is locked in the web interface.
Further, locking a system *does not* restrict the number of users who can access the system via the web interface. If you wish to restrict access to the system, associate that system with a System Group and assign it a System Group Administrator. Refer to Section 6.4.3, “System Groups —” for more information about System Groups.

It is also possible to lock multiple systems via the System Set Manager. Refer to Section 6.4.4.11.4, “System Set Manager ⇒ Misc ⇒ Lock Systems —” to learn how to do so.

— OSA status is also displayed for client systems registered to a Satellite that have a Provisioning

entitlement and have enabled OSA.

Push enables Satellite customers to immediately initiate tasks on Provisioning-entitled system rather than wait for those systems to check in with RHN. Scheduling actions through push is identical to the process of scheduling any other action, except that the task begins immediately instead of waiting the set interval.

In addition to the configuration of the Satellite, each client system to receive pushed actions must have the **osad** package installed and its service started. Refer to the *Enabling Push to Clients* section of the *RHN Satellite Server 5.0.0 Installation Guide* for details.

Subscribed Channels

Base Channel

The first line indicates the base channel to which this client is subscribed. The base channel should match the operating system of the system.

Child Channels

The subsequent lines of text, which depend from the base channel, are child channels. Examples are the **Red Hat Network Tools** channel and the **RHEL AS Extras** channel.

Note

The final link under **Subscribed Channels** is the **Alter Channel subscriptions** link. Click on this link to select from the available base and child channels for this system. When finished making selections, click the **Change Subscriptions** button to confirm the changes.

System Properties

Profile Name

This editable name for the system profile is set to the system's hostname by default. It serves to distinguish this system profile from others.

Entitlement

The base entitlement currently applied to this system.

Notifications

Indicates the the notification options for this system. You can choose whether you wish to receive email notifying you of available errata updates for this system. In addition, you may choose to include Management-entitled systems in the daily summary email.

Auto Errata Update

Indicates whether this system is configured to accept updates automatically.

Description

This information is automatically generated at registration. You can edit this to include any

information you wish.

Location

If entered, this field displays the physical address of the system.

The final link on the page is **Edit these properties**. Clicking this link opens the **System Details ⇒ Properties** subtab. On this page, edit any text you choose, then click the **Update Properties** button to confirm.

6.4.2.9.1.2. System Details ⇒ Details ⇒ Properties

This subtab allows you to alter the following basic properties of your system:

Profile Name

By default, this is the hostname of the system. You can however alter the profile name to anything that allows you to distinguish this profile from others.

Base Entitlement

Select a base channel for the system from the available base entitlements.

Add-on entitlements

If available, apply a Monitoring or Provisioning entitlement to the system.

Notifications

Toggle whether notifications about this system are sent and whether this system is included in the daily summary. (By default, all Management and Provisioning systems are included in the summary.) This setting keeps you abreast of all advisories pertaining to the system. Anytime an update is produced and released for the system, a notification is sent via email.

The daily summary reports system events that affect packages, such as scheduled Errata Updates, system reboots, or failures to check in. In addition to including the system here, you must choose to receive email notification sin the **Your Preferences** page of the **Your RHN** category.

Auto-errata update

If this box is checked, available errata are automatically applied to the system when it checks in. This action takes place without user intervention. Customers should note that Red Hat does not recommend the use of the auto-update feature for production systems because conflicts between packages and environments can cause system failures. The Red Hat Network Daemon must be enabled on the system for this feature to work.

Description

By default, this text box records the operating system, release, and architecture of the system when it first registers. You may edit this information to include anything you like.

The remaining fields record the physical address at which the system is stored. To confirm any changes

to these fields, click the **Update Properties** button.

Note

Many of these properties can be set for multiple systems at once through the System Set Manager interface. Refer to Section 6.4.4, “System Set Manager — ” for details.

6.4.2.9.1.3. System Details ⇒ Details ⇒ Remote Command —

This subtab allows you to run a remote command on the system if the system possesses a Provisioning entitlement. Before doing so, you must first configure the system to accept such commands.

- First, subscribe the system to the RHN Tools channel and use **up2date** to install the **rhncfg**, **rhncfg-client**, and **rhncfg-actions** packages.

```
up2date rhncfg rhncfg-client rhncfg-actions
```

- Log into the system as root and add the following file to the local RHN configuration directory: **allowed-actions/scripts/run**.
  - Create the necessary directory on the target system:

```
mkdir -p /etc/sysconfig/rhn/allowed-actions/script
```

  - Create an empty **run** file in that directory to act as a flag to RHN signaling permission to allow remote commands:

```
touch /etc/sysconfig/rhn/allowed-actions/script/run
```

Once the setup is complete, refresh the page in order to view the text fields for remote commands. You may then identify a specific user, group, and timeout period, as well as the script itself on this page. Select a date and time to begin attempting the command, and click **Schedule Remote Command**.

6.4.2.9.1.4. System Details ⇒ Details ⇒ Reactivation —

An activation key specific to this System Profile. Reactivation keys, available only for systems that have a Provisioning entitlement, include this system's ID, history, groups, and channels. This key can then be used only once with the **rhnreg_ks** command line utility to re-register this system and regain all Red Hat Network settings. Refer to Section 2.5, “Registering with Activation Keys” for instructions. Unlike typical activation keys, which are not associated with a specific system ID, keys created here do not show up within the **Activation Keys** page.

Warning

When kickstarting a system with its existing RHN profile, the kickstart profile uses the system-specific activation key created here to re-register the system and return its other RHN settings. For this reason, you should not regenerate, delete, or use this key (with **rhnreg_ks**) while a profile-based kickstart is in progress. If you do, the kickstart will fail.

6.4.2.9.1.5. System Details ⇒ Details ⇒ Hardware

This subtab provides detailed information about the system, including networking, BIOS, storage, and other devices. This appears only if you selected to include the hardware profile for this machine during registration. If the hardware profile looks incomplete or outdated, click the **Schedule Hardware Refresh** button to schedule a Hardware Profile update for your system. The next time the RHN Daemon connects to RHN, it will update your System Profile with the latest list of hardware.

6.4.2.9.1.6. System Details ⇒ Details ⇒ Notes

This subtab provides a place to create notes about the system. To add a new note, click the **create new note** link, type a subject and details, and click the **Create** button. To modify a note, click on its subject in the list of notes, make your changes, and click the **Update** button. To remove a note, click on its subject in the list of notes and then click the **delete note** link.

6.4.2.9.1.7. System Details ⇒ Details ⇒ Custom Info —

This subtab, available for systems with a Provisioning entitlement, provides completely customizable information about the system. Unlike **Notes**, **Custom Info** is structured, formalized, and can be searched upon. Before you can provide custom information about a system, you must first have **Custom Information Keys**. This is done via the **Custom System Info** page, available from the left navigation bar. Refer to Section 6.4.8, “Custom System Info — ” for instructions.

Once you have created one or more Keys, you may assign a value for this system by select the **create new value** link. Click the name of the key in the resulting list and enter a value for it in the **Description** field, then click the **Update Key** button.

6.4.2.9.1.8. System Details ⇒ Details ⇒ Proxy

Activates an RHN Proxy Server. This tab is only available for Provisioning-entitled systems. Select a version of RHN Proxy Server and click the **Activate Proxy** button to begin the installation and activation process. For detailed information, refer to the *RHN Proxy Server Guide* and the *Client Configuration Guide*.

6.4.2.9.1.9. System Details ⇒ Details ⇒ Satellite

Displays the certificate of an active Red Hat Network. You can deactivate an old certificate here and upload a new one if necessary. This tab requires a Provisioning entitlement. For detailed information on activating a Satellite, refer to the *RHN Satellite Installation Guide*.

6.4.2.9.2. System Details ⇒ Software

This tab and its accompanying subtabs allow you to manage the software of the system: errata, packages and package profiles, and software channel memberships.

6.4.2.9.2.1. System Details ⇒ Software ⇒ Errata

This subtab contains a list of Errata Alerts applicable to the system. Refer to Section 6.1.3, “Errata Alert Icons” for meanings of the icons on this tab. To apply updates, select them and click the **Apply Errata** button. Double-check the updates to be applied on the confirmation page, then click the **Confirm** button. After confirming, the action is added to the **Pending Actions** list under **Schedule**. Errata that have been scheduled cannot be selected for update. In the place of a checkbox is a clock icon that, when clicked, takes you to the **Action Details** page.

To help users determine whether an update has been scheduled, a **Status** column exists within the Errata table. Possible values are: None, Pending, Picked Up, Completed, and Failed. This column

identifies only the latest action related to an Erratum. For instance, if an action fails and you reschedule it, this column shows the status of the Erratum as Pending only (with no mention of the previous failure). Clicking a status other than None takes you to the **Action Details** page. This column corresponds to the one on the **Affected Systems** tab of the **Errata Details** page.

6.4.2.9.2.2. System Details ⇒ Software ⇒ Packages

This subtab allows you to manage the packages on the system.

— When selecting packages to install, upgrade, or remove, Provisioning customers have the option of running a remote command automatically before or after the package installation. Refer to Section 6.4.2.9.1.3, “System Details ⇒ Details ⇒ Remote Command — ” for more information.

Packages

The default display of the **Packages** tab describes the options available to you and provides the means to update your package list. To update or complete a potentially outdated list, possibly due to the manual installation of packages, click the **Update Package List** button on the bottom right-hand corner of this page. The next time the RHN Daemon connects to RHN, it updates your System Profile with the latest list of installed packages.

List/Remove

Lists installed packages from the system's software System Profile and enables you to remove them. Click on a package name to view its **Package Details** page. To delete packages from the system, select their checkboxes and click the **Remove Packages** button on the bottom right-hand corner of the page. A confirmation page appears with the packages listed. Click the **Confirm** button to remove the packages.

Upgrade

Displays a list of packages that have a new version available based on the package versions in the channels for the system. Click on the latest package name to view its **Package Details** page. To upgrade packages immediately, select them and click the **Upgrade Packages** button. To download the packages as a .tar file, select them and click the **Download Packages** button.

Install

Enables you to install new packages on the system from the available channels. Click on the package name to view its **Package Details** page. To install packages, select them and click the **Install Selected Packages** button.

Verify

Validates the packages installed on the system against its RPM database. This is the equivalent of running **rpm -V**. Specifically, this tab allows you to compare the metadata of the system's packages with information from the database, such as MD5 sum, file size, permissions, owner, group and type. To verify a package or packages, select them, click the **Verify Selected Packages** button, and confirm this action. Once finished, you can view the results by selecting this action within the **History** subtab under **Events**.

Profiles

Gives you the ability to compare the packages on this system with the packages of stored profiles and other Management and Provisioning systems. To make the comparison with a stored profile, select that profile from the pulldown menu and click the **Compare** button. To make the comparison with another system, select it from the associated pulldown menu and click the **Compare** button. To create a stored profile based upon the existing system, click the **Create System Profile** button, enter any additional information you desire, and click the **Create Profile** button. These profiles are kept within the **Stored Profiles** page linked from the left navigation bar.

— Once package profiles have been compared, Provisioning customers have the ability to synchronize the packages of the selected system with the package manifest of the compared profile. Note that this action may delete packages on the system not in the profile, as well as install packages from the profile. To install specific packages, select the checkboxes of packages from the profile. To remove specific packages already installed on the system itself, select the checkboxes of packages showing a difference of **This system only.** To synchronize fully the system's packages with the compared profile, select the master checkbox at the top of the column. Then click the **Sync Packages to** button. On the confirmation screen, review the changes, select a time frame for the action, and click the **Schedule Sync** button.

6.4.2.9.2.3. System Details ⇒ Software ⇒ Software Channels

Software channels provide a well-defined method to determine which packages should be available to a system for installation or upgrade based upon its operating systems, packages, and functionality. Click a channel name to view its **Channel Details** page. To modify the child channels associated with this system, use the checkboxes next to the channels and click the **Change Subscriptions** button. You will receive a success message or be notified of any errors. To change the system's base channel, select the new one from the pulldown menu and click the **Modify Base Channel** button. Refer to Section 6.6.1, “Software Channels” for more information.

6.4.2.9.3. System Details ⇒ Configuration —

This tab and its subtabs, which do not appear without a Provisioning entitlement, assist in managing the configuration files associated with the system. These configuration files may be managed solely for the current system, or may be distributed widely via a Configuration Channel. The following section describe these and other available options on the **System Details** ⇒ **Configuration** subtabs.

Note

To manage the configuration of a system, it must have the latest **rhncfg*** packages installed. Refer to Section 6.6.6.1, “Preparing Systems for Config Management” for instructions on enabling and disabling scheduled actions for a system.

This section is available to normal users with access to systems that have configuration management enabled. Like software channels, configuration channels store files to be installed on systems. While software updates are provided by RHN, configuration files are managed solely by you. Also unlike software packages, various versions of configuration files may prove useful to a system at any given time. Remember, only the latest version can be deployed.

6.4.2.9.3.1. System Details ⇒ Configuration ⇒ Overview

This subtab provides access to the configuration statistics of your system and to the most common tasks used to manage configuration files. You may change the settings listed under Configuration Stats by clicking on the blue text for that setting. Alternatively, you may perform any of the common configuration management tasks listed on the right of the screen by clicking one of the links.

6.4.2.9.3.2. System Details ⇒ Configuration ⇒ Managed Files

This subtab lists all configuration files currently associated with the system.

Filename

This column shows both the name and the deployment path for this file.

Revision

This column increments any time you make a change to the managed file.

From Config Channel

This column indicates the name of the channel that contains the file, or displays **`(system override)`** for files available to this system only.

Overrides

If this configuration file overrides another, the overridden file is listed in this column along with its host channel.

If you wish to deploy any of these files to the client system, overwriting any changes that have been made locally, check the box to the left of the file and click the **`Deploy Configuration`** button. On the following screen, choose a deployment time and click the **`Schedule Deploy`** button to confirm.

Note

If you click on the **`Filename`** of a **`(system override)`** file, you can edit its contents.

The **`Overrides`** column identifies the config file from which channel will apply if the system is unsubscribed from the config channel that provides the file now. For instance, if a system has '/etc/foo' from channel 'bar' and '/etc/foo' from channel 'baz' is in the Overrides column, then unsubscribing from channel 'bar' will mean that the file from channel 'baz' will be applicable. Also, if nothing is in the 'Overrides' column for a given file path, then unsubscribing from the channel providing the file will mean that the file is no longer managed (though it will *not* remove the file from the system).

6.4.2.9.3.3. System Details ⇒ Configuration ⇒ Compare Files

This subtab compares a configuration file as stored on the Satellite with the file as it exists on the client. (It does not, for example, compare versions of the same file stored in different channels.) Select the files to be diffed, click the **`Compare Files`** button, select a time to perform the diff, and click the **`Schedule Compare`** button to confirm. After the diff has been performed, you may return to this page to view the results.

6.4.2.9.3.4. System Details ⇒ Configuration ⇒ Manage Configuration Channels

This subtab allows you to subscribe to and rank configuration channels that may be associated with the system, lowest first. Enter numbers in the **Rank** fields to establish the order in which channels are used. Channels with no numeric value are not associated with the system. This system's local configuration channel will always override all other channels for this system and therefore cannot have its rank adjusted from 1. All other channels are created in the **Manage Config Channels** interface within the **Channels** category. Refer to Section 6.6.6, “Manage Config Channels — ” for instructions. When satisfied, click **Update**.

6.4.2.9.3.5. System Details ⇒ Configuration ⇒ Local Overrides

This subtab displays the default configuration files for the system and allows you to manage them. If no files exist, you may use the **add files**, **upload files**, and **add directories** links within the page description to associate files with this system. These tabs correspond to those within the **Configuration Channel Details** page, affecting your entire organization and available only to Configuration Administrators. Refer to Section 6.6.6.5, “Configuration Channel Details — ” for more information.

If a file exists, click its name to go to the **Configuration File Details** page. Refer to Section 6.6.6.6, “Configuration File Details — ” for instructions. To replicate the file within a config channel, select its checkbox, click the **Copy to Config Channel** button, and select the destination channel. To remove a file, select it and click **Delete Selected Files**.

6.4.2.9.3.6. System Details ⇒ Configuration ⇒ Sandbox

This subtab allows you to manipulate configuration files without deploying them. This sandbox provides you with an area in which to experiment with files without affecting your systems. To add files, click the **import new files** link, enter the path to the file on you local system, and click the **Add** button. Select the **Import Files** button to confirm.

6.4.2.9.4. System Details ⇒ Provisioning —

This tab and its subtabs allow you to schedule and monitor kickstarts and to return your system to a previous state. Kickstart is a Red Hat utility that allows you to automate the reinstallation of a system. Snapshots keep a record of every change to a Provisioning system and allow you to "undo" those changes at will. Both features are described in the sections that follow.

6.4.2.9.4.1. System Details ⇒ Provisioning ⇒ Kickstart —

This subtab is further divided into **Session Status**, which tracks the progress of previously scheduled kickstarts, and **Schedule**, which allows you to configure and schedule a kickstart for this system.

Schedule

This subtab allows you to schedule the selected system for kickstart. Choose from the list of available kickstart profiles, select a time for the kickstart to begin, and click the **Schedule Kickstart and Finish** button to begin the kickstart. You may first alter kickstart settings by clicking the **Advanced Configuration** button.

Note

You must first create a kickstart profile before it appears on this subtab. If you have not created any profiles, refer to Section 6.4.9.3, “Create a New Kickstart Profile” before scheduling a kickstart for a system.

Session Status

If you have scheduled a kickstart, this subtab shows the progress of the kickstart. The provided details include the kickstart profile used, its state, the next action and the number of requested packages. Kickstarts that do not complete within approximately two hours are marked **Kickstart Failed**. The page refreshes itself periodically, or you can force a refresh using your browser's controls.

6.4.2.9.4.2. System Details ⇒ Provisioning ⇒ Snapshots —

Snapshots enable you to roll back the system's package profile, configuration files, and RHN settings. Snapshots are captured whenever an action takes place on a Provisioning-entitled system. The **Snapshots** subtab lists all snapshots for the system , including the reason the snapshot was taken, the time it was taken, and the number of tags applied to each snapshot. To revert to a previous configuration, click the **Reason** of the snapshot taken and review the potential changes on the provided subtabs, starting with **Rollback**.

Each subtab provides the specific changes that will be made to the system during the rollback:

- group memberships
- channel subscriptions
- installed packages
- configuration channel subscriptions
- configuration files
- snapshot tags

When satisfied with the reversion, return to the **Rollback** subtab and click the **Rollback to Snapshot** button. To see the list again, click **Return to snapshot list**.

6.4.2.9.4.3. System Details ⇒ Provisioning ⇒ Snapshot Tags —

Provides a means to add meaningful descriptions to your most recent system snapshot. This can be used to indicate milestones, such as a known working configuration or a successful upgrade. To tag the most recent snapshot, click **create new system tag**, enter a descriptive term in the **Tag name** field, and click the **Tag Current Snapshot** button. You may then revert using this tag directly by clicking its name in the Snapshot Tags list. To delete tags, select their checkboxes, click **Remove Tags**, and confirm the action.

6.4.2.9.5. System Details ⇒ Virtualization

This is tab allows you to create a new virtual guest on a host system or allows you to change the status of virtual guests.

The **Virtualization** tab has two subtabs, **Details** and **Kickstart**. These tabs appear the same

for both virtual hosts and guests, but the functionality only makes sense for virtual hosts. It is not possible to create a guest system that runs on another guest system.

6.4.2.9.5.1. System Details ⇒ Virtualization ⇒ Details

Details is the default tab. For host systems, it presents a table of the host system's virtual guests. For each guest system, the following information is provided:

Status

This field indicates whether the virtual system is running, paused, stopped, or has crashed.

Updates

This field indicates whether errata applicable to the guest have yet to be applied.

Base Software Channel

This field indicates the Base Channel to which the guest is subscribed.

Tip

If a guest system has not registered to the Satellite, this information appears as plain text in the table.

If you have System Group Administrator responsibilities assigned for your guest systems, it is possible that a user could see the message **You do not have permission to access this system** within the table. This is because it is possible to assign virtual guests on a single host to multiple System Group Administrators. Only users that have System Group Administrator privileges on the host system may create new virtual guests.

6.4.2.9.5.2. System Details ⇒ Monitoring —

This tab is only visible for systems registered to a RHN Satellite with Monitoring enabled and that are Monitoring entitled. It displays all of the probes monitoring the system. The **State** column shows icons representing the status of each probe. Refer to Section 6.9, “Monitoring — ” for descriptions of these states. Clicking the **Probe Description** takes you to its **Current State** page. The **Status String** column displays the last message received from the probe.

To add a probe to the system, click the **create new probe** link at the top-right corner of the page and complete the fields on the following page. Refer to Section 7.5.1, “Managing Probes” for detailed instructions.

Once the probe has been added, you must reconfigure your Monitoring infrastructure to recognize it. Refer to Section 6.9.4, “Scout Config Push — ” for details. After the probe has run, its results become available on the **Current State** page. Refer to Section 6.9.1.7, “Current State — ” for details.

To remove a probe from a system, click on the name of the probe, then click the **delete probe** link in the upper right corner. Finally, click the **Delete Probe** button to complete the process.

6.4.2.9.5.3. System Details ⇒ Groups —

This tab and its subtabs allow you to manage the system's group memberships.

6.4.2.9.5.3.1. System Details ⇒ Groups ⇒ List/Leave —

This subtab lists groups to which the system belongs and enables you to cancel those associations. Only System Group Administrators and Organization Administrators can remove the system from groups. Non-admins just see a **`Review this system's group membership`** page. To remove the system from groups, select the groups' checkboxes and click the **`Leave Selected Groups`** button. Click on a group's name to go to its **`System Group Details`** page. Refer to Section 6.4.3.3, “System Group Details — ” for more information.

6.4.2.9.5.3.2. System Details ⇒ Groups ⇒ Join —

Lists groups that the system may be subscribed to. Only System Group Administrators and Organization Administrators can add the system to groups. Non-admins see a **`Review this system's group membership`** page. To add the system to groups, select the groups' checkboxes and click the **`Join Selected Groups`** button.

6.4.2.9.5.4. System Details ⇒ Events

Displays past, current, and scheduled actions on the system. You may cancel pending events here. The following sections describe the **`Events`** sub-tabs and the features they offer.

6.4.2.9.5.4.1. System Details ⇒ Events ⇒ Pending

Lists events that are scheduled but have not begun. A prerequisite action must complete successfully before a given action is attempted. If an action has a prerequisite, no checkbox is available to cancel that action. Instead, a checkbox appears next to the prerequisite action; canceling the prerequisite action causes the action in question to fail.

Actions can be chained in this manner so that action 'a' requires action 'b' which requires action 'c'. Action 'c' is the first one attempted and has a checkbox next to it until it is completed successfully - if any action in the chain fails, the remaining actions also fail. To unschedule a pending event, select the event and click the **`Cancel Events`** button at the bottom of the page. The following icons indicate the type of events listed here:

- — Package Event
- — Errata Event
- — Preferences Event
- — System Event

6.4.2.9.5.4.2. System Details ⇒ Events ⇒ History

The default display of the **`Events`** tab lists the type and status of events that have failed, occurred or are occurring. To view details of an event, click its summary in the **`System History`** list. To again view the table, click **`Return to history list`** at the bottom of the page.

6.4.3. System Groups —

The **`System Groups`** page allows all RHN Management and Provisioning users to view the **`System Groups`** list. Only System Group Administrators and Organization Administrators may perform the

following additional tasks:

1. Create system groups. (Refer to Section 6.4.3.1, “Creating Groups”.)
2. Add systems to system groups. (Refer to Section 6.4.3.2, “Adding and Removing Systems in Groups”.)
3. Remove systems from system groups. (Refer to Section 6.4.2.9, “System Details”.)
4. Assign system group permissions to users. (Refer to Section 6.8, “Users — ”.)

The **System Groups** list displays all of your system groups.

The **System Groups** list contains several columns for each group:

- **Select** — These checkboxes enable you to add systems in groups to the **System Set Manager**. To select groups, mark the appropriate checkboxes and click the **Update** button below the column. All systems in the selected groups are added to the **System Set Manager**. You can then use the **System Set Manager** to perform actions on them simultaneously. It is possible to select only those systems that are members of all of the selected groups, excluding those systems that belong only to one or some of the selected groups. To do so, select them and click the **Work with Intersection** button. To add all systems in all selected groups, select them and click the **Work with Union** button. Each system will show up once, regardless of the number of groups to which it belongs. Refer to Section 6.4.4, “System Set Manager — ” for details.
- **Status** — Shows which type of Errata Alerts are applicable to the group or confirms that it is up-to-date. Clicking on a group's status icon takes you to the **Errata** tab of its **System Group Details** page. Refer to Section 6.4.3.3, “System Group Details — ” for more information.

  The status icons call for differing degrees of attention:
  - — All systems within group are up-to-date
  - — Critical Errata available, update *strongly* recommended
  - — Updates available and recommended
- **Group Name** — The name of the group as configured during its creation. The name should be explicit enough to easily differentiate between it and other groups. Clicking on the name of a group takes you to **Details** tab of its **System Group Details** page. Refer to Section 6.4.3.3, “System Group Details — ” for more information.
- **Systems** — Total number of systems contained by the group. Clicking on the number takes you to the **Systems** tab of the **System Group Details** page for the group. Refer to Section 6.4.3.3, “System Group Details — ” for more information.
- **Use in SSM** — Clicking the **Use Group** button in this column loads the group from that row and launches the **System Set Manager** immediately. Refer to Section 6.4.4, “System Set Manager — ” for more information.

6.4.3.1. Creating Groups

To add a new system group, click the **create new group** button at the top-right corner of the page. Type a name and description and click the **Create Group** button. Make sure you use a name that clearly sets this group apart from others. The new group will appear in the **System Groups** list.

6.4.3.2. Adding and Removing Systems in Groups

Systems can be added and removed from system groups in two places: the **Target Systems** tab of

the **System Group Details** page and the **Groups** tab of the **System Details** page. The process is similar in both instances. Select the systems to be added or removed and click the **Add Systems** or **Remove Systems** button.

6.4.3.3. System Group Details —

At the top of each **System Group Details** page are two links: **work with group** and **delete group**. Clicking **delete group** deletes the System Group and should be used with caution. Clicking **Work with Group** functions similarly to the **Use Group** button from the **System Groups** list in that it loads the group's systems and launches the **System Set Manager** immediately. Refer to Section 6.4.4, "System Set Manager — " for more information.

The **System Group Details** page is broken down into tabs:

6.4.3.3.1. System Group Details ⇒ Details —

Provides the group name and group description. To change this information, click **Edit Group Properties**, make your changes in the appropriate fields, and click the **Modify Details** button.

6.4.3.3.2. System Group Details ⇒ Systems —

Lists systems that are members of the system group. Clicking links within the table takes you to corresponding tabs within the **System Details** page for the associated system. To remove systems from the group, select the appropriate checkboxes and click the **Remove from group** button on the bottom of the page. Clicking it does not delete systems from RHN entirely. This is done through the **System Set Manager** or **System Details** pages. Refer to Section 6.4.4, "System Set Manager — " or Section 6.4.2.9, "System Details", respectively.

6.4.3.3.3. System Group Details ⇒ Target Systems —

Target Systems — Lists all systems in your organization. This tab enables you to add systems to the specified system group. Select the systems using the checkboxes to the left and click the **Add Systems** button on the bottom right-hand corner of the page.

6.4.3.3.4. System Group Details ⇒ Errata —

List of relevant Errata for systems in the system group. Clicking the Advisory takes you to the **Details** tab of the **Errata Details** page. (Refer to Section 6.5.2.2, "Errata Details" for more information.) Clicking the Affected Systems number lists all of the systems addressed by the Errata. To apply the Errata Updates in this list, select the systems and click the **Apply Errata** button.

6.4.3.3.5. System Group Details ⇒ Admins —

List of all organization users that have the ability to manage the system group. Organization Administrators are clearly identified. System Group Administrators are marked with an asterisk (*). To change the system group's users, select and unselect the appropriate checkboxes and click the **Update** button.

6.4.4. System Set Manager —

Many actions performed for individual systems through the System Details page may be performed for multiple systems via the System Set Manager, including:

- Apply Errata updates
- Upgrade packages to the most recent versions available
- Add/remove systems to/from system groups
- Subscribe/unsubscribe systems to/from channels
- Update system profiles
- Modify system preferences such as scheduled download and installation of packages
- Kickstart several Provisioning-entitled systems at once
- Set the subscription and rank of configuration channels for Provisioning-entitled systems
- Tag the most recent snapshots of your selected Provisioning-entitled systems
- Revert Provisioning-entitled systems to previous snapshots
- Run remote commands on Provisioning-entitled systems

Before performing actions on multiple systems, select the systems you wish to modify. To do so, click the **`List the systems`** link, check the boxes to the left of the systems you wish to select, and click the **`Update List`** button.

You can access the System Set Manager in three ways:

1. Click the **`System Set Manager`** link in the left gray navigation area.
2. Click the **`Use Group`** button in the **`System Groups`** list.
3. Check the **`Work with Group`** link on the **`System Group Details`** page.

6.4.4.1. System Set Manager ⇒ Overview —

Description of the various options available to you in the remaining tabs.

6.4.4.2. System Set Manager ⇒ Systems —

List of systems now selected. To remove systems from this set, select them and click the **`Remove`** button.

6.4.4.3. System Set Manager ⇒ Errata —

List of Errata Updates applicable to the current system set. Click the number in the Systems column to see to which systems in the System Set Manager the given Errata applies. To apply updates, select the Errata and click the **`Apply Errata`** button.

6.4.4.4. System Set Manager ⇒ Packages —

Options to modify packages on the system within the following subtabs (Click the number in the Systems column to see to which systems in the System Set Manager the given package applies):

— When selecting packages to install, upgrade, or remove, Provisioning customers have the option of running a remote command automatically before or after the package installation. Refer to Section 6.4.2.9.1.3, “System Details ⇒ Details ⇒ Remote Command — ” for more information.

6.4.4.4.1. System Set Manager ⇒ Packages ⇒ Upgrade —

A list of all the packages installed on the selected systems that might be upgraded. Systems must be subscribed to a channel providing the package for the system to be able to upgrade the package. If multiple versions of a package appear, note that only the latest version available to each system is

upgraded on that system. Select the packages to be upgraded, then click the **Upgrade Packages** button.

6.4.4.4.2. System Set Manager ⇒ Packages ⇒ Install —

A list of channels from which you may retrieve packages. This list includes all channels to which systems in the set are subscribed; a package is installed on a system only if the system is subscribed to the channel from which the package originates. Click on the channel name and select the packages from the list. Then click the **Install Packages** button.

6.4.4.4.3. System Set Manager ⇒ Packages ⇒ Remove —

A list of all the packages installed on the selected systems that might be removed. Multiple versions appear if systems in the System Set Manager have more than one version installed. Select the packages to be deleted, then click the **Remove Packages** button.

6.4.4.5. System Set Manager ⇒ Verify

A list of all installed package whose contents, MD5 sum, and other details may be verified. At the next check in, the verify event issues the command **rpm --verify** for the specified package. If there are any discrepancies, they are displayed in the System Details page for each system.

Select the checkbox next to all packages to be verified, then click the **Verify Packages** button. On the next page, select either **Schedule actions ASAP** or choose a date and time for the verification, then click the **Schedule Verifications** button.

6.4.4.6. System Set Manager ⇒ Patches

Tools to manage patches to Solaris clients. Patches may be installed or removed via the subtabs.

6.4.4.7. System Set Manager ⇒ Patch Clusters

Tools to manage patch clusters for Solaris clients. Patches may be installed or removed via the subtabs.

6.4.4.8. System Set Manager ⇒ Groups —

Tools to create groups and manage group membership. These functions are limited to Organization Administrators and System Group Administrators. To add a new group, click **create new group** on the top-right corner. In the resulting page, type its name and description in the identified fields and click the **Create Group** button. To add or remove the selected systems in any of the system groups, toggle the appropriate radio buttons and click the **Alter Membership** button.

6.4.4.9. System Set Manager ⇒ Channels —

Options to manage channel associations through the following subtabs:

6.4.4.9.1. System Set Manager ⇒ Channels ⇒ Channel Subscriptions —

To subscribe or unsubscribe the selected systems in any of the channels, toggle the appropriate radio buttons and click the **Alter Subscriptions** button. Keep in mind that subscribing to a channel uses a channel entitlement for each system in the selected group. If too few entitlements are available, some systems fail to subscribe. Systems must subscribe to a base channel before subscribing to a child channel.

6.4.4.9.2. System Set Manager ⇒ Channels ⇒ Config Channels —

Like the options within the **System Details ⇒ Channels ⇒ Configuration** tab, the subtabs here can be used to subscribe the selected systems to configuration channels and deploy and compare the configuration files on the systems. The channels are created in the **Manage Config Channels** interface within the **Channels** category. Refer to Section 6.6.6, "Manage Config Channels — " for channel creation instructions.

To manage the configuration of a system, install the latest **rhncfg*** packages. Refer to Section 6.6.6.1, "Preparing Systems for Config Management" for instructions on enabling and disabling scheduled actions for a system.

6.4.4.9.2.1. System Set Manager ⇒ Channels ⇒ Config Channels ⇒ Deploy —

Use this subtab to distribute configuration files from your central repository on RHN to each of the selected systems. The table lists the configuration files associated with any of the selected systems. Clicking its system count displays the systems already subscribed to the file.

To subscribe the selected systems to the available configuration files, select the checkbox for each desired file. When done, click **Deploy Configuration** and schedule the action. Note that the files deployed are of the latest version at the time of scheduling and do not account for versions that may appear before the action takes place.

6.4.4.9.2.2. System Set Manager ⇒ Channels ⇒ Config Channels ⇒ Diff —

Use this subtab to validate configuration files on the selected systems against copies in your central repository on RHN. The table lists the configuration files associated with any of the selected systems. Clicking its system count displays the systems already subscribed to the file.

To compare the configuration files deployed on the systems with those in RHN, select the checkbox for each file to be validated. Then click **Analyze Differences** and schedule the action. Note that the files compared are of the latest version at the time of scheduling and do not account for versions that may appear before the action takes place. Find the results within the main **Schedule** category or within the **System Details ⇒ Events** tab.

6.4.4.9.2.3. System Set Manager ⇒ Channels ⇒ Config Channels ⇒ Subscriptions —

Subscribe systems to configuration channels according to order of preference. This tab is available only to Organization Administrators and Configuration Administrators. Enter a number in the **Rank** column to subscribe to a channel. Channels are accessed in the order of their rank, starting from the number 1. Channels not assigned a numeric value are not associated with the selected systems. Your local configuration channel always overrides all other channels. Once you have established the rank of the config channels, you must decide how they are applied to the selected systems.

The three buttons below the channels reflect your options. Clicking **Add with Highest Rank** places all the ranked channels before any other channels to which the selected systems are currently subscribed. Clicking **Add with Lowest Rank** places the ranked channels after those channels to which the selected systems are currently subscribed. Clicking **Replace Existing Config Channels** removes any existing association and starts cleanly with the ranked channels, leaving every system with the same config channels in the same order.

In the first two cases, if any of the newly ranked config channels is already in a system's existing config channel list, the duplicate channel is removed and replaced according to the new rank, effectively reordering the system's existing channels. When such conflicts exist, you are presented with a

confirmation page to ensure the intended action is correct. When the change has taken place, a message appears at the top of the page indicating the update was successful.

6.4.4.9.3. System Set Manager ⇒ Channels ⇒ Base Channel Alteration —

Channel Administrators may change the base channels to which the selected systems are subscribed via this subtab. The default Red Hat base channel selection in the pulldown menu subscribes the system to whichever Red Hat-provided base channel represents the operating system installed on the system. Systems are unsubscribed from all channels and subscribed to the new base channels. For this reason, this should be done with caution. Select the new base channel from the pulldown menus and click the **`Change Base Channels`** button.

6.4.4.10. System Set Manager ⇒ Provisioning —

Options for provisioning systems through the following subtabs:

6.4.4.10.1. System Set Manager ⇒ Provisioning ⇒ Kickstart —

Use this subtab to re-install Red Hat Enterprise Linux on the selected Provisioning-entitled systems. To schedule kickstarts for these systems, select a distribution, identify the type (IP address or manual), and click **`Continue`**. Finish choosing from the options available on the subsequent screen. If any of the systems connect to RHN via a RHN Proxy Server, choose either the **`Preserve Existing Configuration`** radio button or the **`Use RHN Proxy`** radio button. If you choose to kickstart through a RHN Proxy Server, select from the available Proxies listed in the drop-down box beside the **`Use RHN Proxy`** radio button. All of the selected systems will kickstart through the selected Proxy. Click the **`Schedule Kickstart`** button to confirm your selections. When the kickstarts for the selected systems are successfully scheduled, the web interface returns you to the System Set Manager page.

6.4.4.10.2. System Set Manager ⇒ Provisioning ⇒ Tag Systems —

Use this subtab to add meaningful descriptions to the most recent snapshots of your selected systems. To tag the most recent system snapshots, enter a descriptive term in the **`Tag name`** field and click the **`Tag Current Snapshots`** button.

6.4.4.10.3. System Set Manager ⇒ Provisioning ⇒ Rollback —

Use this subtab to rollback selected Provisioning-entitled systems to previous snapshots marked with a tag. Click the name of the tag, verify the systems to be reverted, and click the **`Rollback Systems`** button.

6.4.4.10.4. System Set Manager ⇒ Provisioning ⇒ Remote Command —

Use this subtab to issue remote commands on selected Provisioning-entitled systems. First create a **`run`** file on the client systems to allow this function to operate. Refer to the description of the **`Configuration`** subtab of the **`Channels`** tab for instructions. You may then identify a specific user, group, timeout period, and the script on this page. Select a date and time to perform the command, and click **`Schedule Remote Command`**.

6.4.4.11. System Set Manager ⇒ Misc —

`Misc` — Update System Profiles and preferences for the system set through the following links:

6.4.4.11.1. System Set Manager ⇒ Misc ⇒ System Profile Updates —

Click **Update Hardware Profile** followed by the **Confirm Refresh** button to schedule a hardware profile update. Clicking **Update Package Profile**,followed by the **Confirm Refresh** button schedules a package profile update.

6.4.4.11.2. System Set Manager ⇒ Misc ⇒ Custom System Information —

Click **Set a custom value for selected systems** followed by the name of a key to allow you to provide values for all selected systems. Enter the information and click the **Set Values** button. Click **Remove a custom value from selected systems** followed by the name of a key to allow you to remove values for all selected systems. Click the **Remove Values** button to finalize the deletion.

6.4.4.11.3. System Set Manager ⇒ Misc ⇒ Reboot Systems —

Select the appropriate systems and click the **Reboot Systems** link to set those systems for reboot. To immediately cancel this action, click the **list of systems** link that appears within the confirmation message at the top of the page, select the systems, and click **Unschedule Action**.

6.4.4.11.4. System Set Manager ⇒ Misc ⇒ Lock Systems —

Select the appropriate systems and click the **Lock Systems** link to prevent the scheduling of any action through RHN that affects the selected systems. This can be reversed by clicking the **Unlock Systems** link.

6.4.4.11.5. System Set Manager ⇒ Misc ⇒ Delete Systems —

Click **Delete System Profiles**, then click the **Confirm Deletions** button to remove the selected profiles permanently.

6.4.4.11.6. System Set Manager ⇒ Misc ⇒ Add or Remove Add-On Entitlements —

Select, via the radio button, whether to **Add**, **Remove**, or make **No Change** in the entitlements of the selected systems. Click the **Change Entitlements** button to confirm your selection.

6.4.4.11.7. System Set Manager ⇒ Misc ⇒ System Preferences —

Toggle the **Yes** and **No** radio buttons and click the **Change Preferences** button to alter your notification preferences for the selected systems. You may apply these preferences to individual systems through the **Properties** subtab of the **System Details** page. Refer to Section 6.4.2.9.1.2, “System Details ⇒ Details ⇒ Properties” for instructions.

- **Receive Notifications of Updates/Errata** — This setting keeps you abreast of all advisories pertaining to your systems. Any time an update is produced and released for a system under your supervision, a notification is sent via email.
- **Include system in Daily Summary** — This setting includes the selected systems in a daily summary of system events. (By default, all Management and Provisioning systems are included in the summary.) These system events are actions that affect packages, such as scheduled Errata Updates, system reboots, or failures to check in. In addition to including the systems here, you must choose to receive email notifications in the **Your Preferences** page of **Your RHN**. Refer to Section 6.3.2, “Your Preferences” for instructions. Note that RHN sends these summaries only to verified email addresses.
- **Automatic application of relevant Errata** — This setting enables the automatic application of Errata Updates to the selected systems. This means packages associated with Errata are updated without any user intervention. Customers should note that Red Hat does not recommend

the use of the auto-update feature for production systems because conflicts between packages and environments can cause system failures.

6.4.5. Advanced Search —

The **System Search** page allows you to search through your systems according to specific criteria. These criteria include custom system information, system details, hardware, devices, interface, networking, packages, and location. The activity selections (Days Since Last Checkin, for instance) can be especially useful in finding and removing outdated System Profiles. Type the keyword, select the criterion to search by, use the radio buttons to identify whether you wish to query all systems or only those loaded in the **System Set Manager**, and click the **Search** button. You may also select the **Invert Result** checkbox to list those systems that do *not* match the criteria selected.

The results appear at the bottom of the page. For details about using the resulting system list, refer to Section 6.4.2, “Systems”.

6.4.6. Activation Keys —

RHN Management and Provisioning customers with the Activation Key Administrator role (including Organization Administrators) can generate activation keys through the RHN website. These keys can then be used to register a Red Hat Enterprise Linux system, entitle the system to an RHN service level and subscribe the system to specific channels and system groups through the command line utility **rhnreg_ks**. Refer to Section 2.5, “Registering with Activation Keys” for instructions on use.

Note

System-specific activation keys created through the **Reactivation** subtab of the **System Details** page are not part of this list because they are not reusable across systems.

6.4.6.1. Managing Activation Keys

To generate an activation key:

1. Select **Systems** => **Activation Keys** from the top and left navigation bars.
2. Click the **create new key** link at the top-left corner.

Warning

In addition to the fields listed below, RHN Satellite customers may also populate the **Key** field itself. This user-defined string of characters can then be supplied with **rhnreg_ks** to register client systems with the Satellite. *Do not insert commas in the key.* All other characters are accepted. Commas are problematic since they are the separator used when including two or more activation keys at once. Refer to Section 6.4.6.2, “Using Multiple Activation Keys at Once — ” for details.

3. Provide the following information:
   - **Description** — User-defined description to identify the generated activation key.
   - **Usage Limit** — The maximum number of registered systems that can be registered to the activation key at any one time. Leave blank for unlimited use. Deleting a system profile reduces the usage count by one and registering a system profile with the key increases the usage

count by one.

- **Base Channel** — The primary channel for the key. Selecting nothing will enable you to select from all child channels, although systems can be subscribed to only those that are applicable.
- **Entitlement** — The service level for the key, either Management or Provisioning. All systems will be subscribed at this level with the key.
- **Universal default** — Whether or not this key should be considered the primary activation key for your organization.

Click **Create Key**.

After creating the unique key, it appears in the list of activation keys along with the number of times it has been used. Note that only Activation Key Administrators can see this list. At this point, you may associate child channels and groups with the key so that systems registered with it automatically subscribe to them.

To change information about a key, such as the channels or groups, click its description in the key list, make your modifications in the appropriate tab, and click the **Update Key** button. To disassociate channels and groups from a key, deselect them in their respective menus by **Ctrl**-clicking their highlighted names. To remove a key entirely, click the **delete key** link in the top-right corner of the edit page.

A system may be set to subscribe to a base channel during registration with an activation key. However, if the activation key specifies a base channel that is not compatible with the operating system of the systems, the registration fails. For example, a Red Hat Enterprise Linux AS v.4 for x86 system cannot register with an Activation Key that specifies a Red Hat Enterprise Linux ES v.4 for x86 base channel. A system is always allowed to subscribe to a custom base channel.

To disable system activations with a key, unselect the corresponding checkbox under the **Enabled** column in the key list. The key can be re-enabled by selecting the checkbox. After making these changes, click the **Update Keys** button on the bottom right-hand corner of the page.

6.4.6.2. Using Multiple Activation Keys at Once —

Provisioning customers should note that multiple activation keys can be included at the command line or in a single kickstart profile. This allows you to aggregate the aspects of various keys without recreating a new key specific to the desired systems, simplifying the registration and kickstart processes while slowing the growth of your key list.

Without this stacking ability, your organization would need at least six activation keys to manage four server groups and subscribe a server to any two groups. Factor in two versions of the operating system, such as Red Hat Enterprise Linux 3 and 4, and you need twice the number of activation keys. A larger organization would need keys in the dozens.

Registering with multiple activation keys requires some caution; conflicts between some values cause registration to fail. Conflicts in the following values do not cause registration to fail, a combination of values is applied: software packages, software child channels, and config channels. Conflicts in the remaining properties are resolved in the following manner:

- base software channels — registration fails
- entitlements — registration fails
- enable config flag — configuration management is set

Do not use system-specific activation keys along with other activation keys; registration fails in this event.

You are now ready to use multiple activation keys at once. This is done with comma separation at the command line with **rhnreg_ks** or in a kickstart profile within the **Post** tab of the **Kickstart Details** page. Refer to Section 2.5, “Registering with Activation Keys” and Section 6.4.9.3, “Create a New Kickstart Profile”, respectively, for instructions.

6.4.7. Stored Profiles —

RHN Provisioning customers can create package profiles through the **Profiles** subtab of the **Packages** tab within the **System Details** page. Those profiles are displayed on the **Stored Profiles** page, where they may be edited and even deleted.

To edit a profile, click its name in the list, alter its name and description, and click the **Update Profile** button. To view software associated with the profile, click the **Packages** subtab. To remove the profile entirely, click **delete stored profile** at the upper-right corner of the page.

6.4.8. Custom System Info —

RHN Provisioning customers may include completely customizable information about their systems. Unlike notes, the information here is more formal and may be searched upon. For instance, you may decide to identify an asset tag for each system. To do this, you must create an **asset** key within the **Custom System Info** page.

Click **create new key** at the upper-right corner of the page. Enter a descriptive label and description, such as **Asset** and **Precise location of each system**, and click the **Create Key**. The key will then show up in the custom info keys list.

Once the key exists, you may assign a value to it through the **Custom Info** tab of the **System Details** page. Refer to Section 6.4.2.9.1.7, “System Details ⇒ Details ⇒ Custom Info —” for instructions.

6.4.9. Kickstart —

To satisfy the provisioning needs of customers, RHN provides this interface for developing kickstart profiles that can be used to install Red Hat Enterprise Linux on either new or already-registered systems. This enables systems to be installed automatically to particular specifications.

Important

If your systems are connected to the central RHN Servers, you will need an external installation tree for each distribution to be kickstarted. This tree can be hosted anywhere that is accessible by the target system via HTTP. If the systems are connected through an RHN Proxy Server, then you may place the installation tree in **/var/www/html/pub/** on the Proxy. RHN Satellites already have a tree for each Red Hat distribution and therefore do not require separate trees. Even if the system connects through an RHN Proxy Server to get to the Satellite, these trees will be available for kickstart. Refer to Section 6.4.9.6, “Kickstart ⇒ Distributions —” for instructions on setting up installation trees.

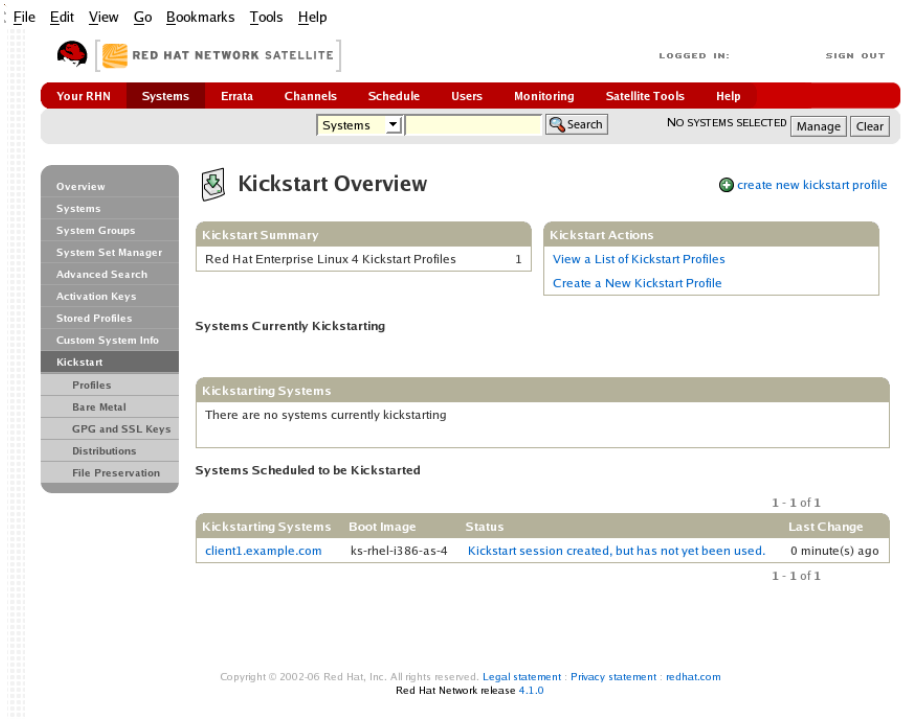


Figure 6.7. Kickstart Overview

This overview page displays the status of kickstart on your client systems: the types and number of profiles you have created and the progress of systems that are scheduled to be kickstarted. In the upper right is the **`Kickstart Actions`** section, which contains a series of links to management actions for your kickstart profiles. Before explaining the various kickstart options that are available from this page, the next section provides some introduction to the subject of kickstart.

6.4.9.1. Introduction to Kickstart

Many system administrators would prefer to use an automated installation method to install Red Hat Enterprise Linux on their machines. To answer this need, Red Hat created the kickstart installation method. Using kickstart, a system administrator can create a single file containing the answers to all the questions that would normally be asked during a typical installation.

Kickstart files can be kept on a single server system and read by individual computers during the installation. This installation method can support the use of a single kickstart file to install Red Hat Enterprise Linux on multiple machines, making it ideal for network and system administrators.

The *Red Hat Enterprise Linux System Administration Guide* contains an in-depth discussion of kickstart and is available here: http://www.redhat.com/docs/manuals/enterprise/.

6.4.9.1.1. Kickstart Explained

When a machine is to receive a network-based kickstart, the following events must occur in this order:

1. After being placed on the network and turned on, the machine's PXE logic broadcasts its MAC address and a request to be discovered.
2. If a static IP address is not being used, the DHCP server recognizes the discovery request and extends an offer of network information needed for the new machine to boot. This includes an IP address, the default gateway to be used, the netmask of the network, the IP address of the TFTP or HTTP server holding the bootloader program, and the full path and file name of that program (relative to the server's root).

3. The machine applies the networking information and initiates a session with the server to request the bootloader program.
4. The bootloader, once loaded, searches for its configuration file on the server from which it was itself loaded. This file dictates which kernel and kernel options, such as the initial RAM disk (initrd) image, should be executed on the booting machine. Assuming the bootloader program is SYSLINUX, this file is located in the **pxelinux.cfg** directory on the server and named the hexadecimal equivalent of the new machine's IP address. For example, a bootloader configuration file for Red Hat Enterprise Linux AS 2.1 should contain:

```
 port 0 prompt 0 timeout 1 default My_Label label My_Label kernel vmlinuz
append ks=http://myrhnsatellite/ initrd=initrd.img network apic
```

5. The machine accepts and uncompresses the init image and kernel, boots the kernel, and initiates a kickstart installation with the options supplied in the bootloader configuration file, including the server containing the kickstart configuration file.
6. This kickstart configuration file in turn directs the machine to the location of the installation files.
7. The new machine is built based upon the parameters established within the kickstart configuration file.

6.4.9.1.2. Kickstart Prerequisites

Although Red Hat Network has taken great pains to ease the provisioning of systems, some preparation is still required for your infrastructure to handle kickstarts. For instance, before creating kickstart profiles, you may consider:

- A DHCP server is not required for kickstarting, but it can make things easier. If you are using static IP addresses, you should select static IP while developing your kickstart profile.
- An FTP server can be used in place of hosting the kickstart distribution trees via HTTP.
- If conducting a bare metal kickstart, you should 1)Configure DHCP to assign required networking parameters and the bootloader program location. 2)Specify within the bootloader configuration file the kernel to be used and appropriate kernel options.

6.4.9.1.3. Building Bootable Kickstart ISOs

While you can schedule a registered system to be kickstarted to a new operating system and package profile, it is also useful to be able to kickstart a system that is not registered with RHN, or does not yet have an operating system installed. One common method of doing this is to create a bootable CD-ROM that is inserted into the target system. When the system is rebooted, it boots from the CD-ROM, loads the kickstart configuration from the RHN Servers or your Satellite, and proceeds to install Red Hat Enterprise Linux according to the kickstart profile you have created.

To do this, copy the contents of **/isolinux** from the first CD-ROM of the target distribution. Then edit the **isolinux.cfg** file to default to 'ks'. Change the 'ks' section to the following template:

```
 label ks kernel vmlinuz append text ks={url} initrd=initrd.img lang=
devfs=nomount ramdisk_size=16438 \ {ksdevice}
```

IP addressed-based kickstart URLs will look something like this:

```
 http://my.sat.server/kickstart/ks/mode/ip_range
```

The kickstart distribution selected by the IP range should match the distribution from which you are building, or errors will occur. {ksdevice} is optional, but looks like:

```
ksdevice=eth0
```

It is possible to change the distribution for a kickstart profile within a family, such as Red Hat Enterprise Linux AS 4 to Red Hat Enterprise Linux ES 4, by specifying the new distribution label. Note that you cannot move between versions (2.1 to 3) or between updates (U1 to U2).

Next, you may customize **isolinux.cfg** further for your needs, such as by adding multiple kickstart options, different boot messages, shorter timeout periods, etc.

Next, create the ISO as described in the *Making an Installation Boot CD-ROM* section of the *Red Hat Enterprise Linux 3 Installation Guide*. Alternatively, issue the command:

```
mkisofs -o file.iso -b isolinux.bin -c boot.cat -no-emul-boot -boot-load-
size 4 \ -boot-info-table -R -J -v -T isolinux/
```

Note that **isolinux/** is the relative path to the directory containing the isolinux files from the distribution CD, while **file.iso** is the output ISO file, which is placed into the current directory.

You may then burn the ISO to CD-ROM. To use the disc (assuming you left the label for the kickstart boot as 'ks'), boot the system and type "ks" at the prompt. When you press **Enter**, the kickstart should begin.

6.4.9.1.4. Integrating Kickstart with PXE

In addition to CD-ROM-based installs, RHN supports kickstarts through a Pre-Boot Execution Environment (PXE). This is less error-prone than CDs, enables kickstarting from bare metal, and integrates with existing PXE/DHCP environments.

To use this method, make sure your systems have network interface cards (NIC) that support PXE, install and configure a PXE server, ensure DHCP is running, and then place the appropriate files on an HTTP server for deployment. Once the kickstart profile has been created, use the URL from the **Kickstart Details** page, as for CD-ROM-based installs.

To obtain specific instructions for conducting PXE kickstarts, refer to the *PXE Network Installations* chapter of the *Red Hat Enterprise Linux 4 System Administration Guide*.

Tip

Upon running the **Network Booting Tool** as described in the Red Hat Enterprise Linux 4: System Administration Guide, ensure that you select "HTTP" as the protocol and include the domain name of the RHN Satellite in the Server field if you intend to use it to distribute the installation files.

The following sections describe the kickstart options available from the **Systems** ⇒ **Kickstart** page.

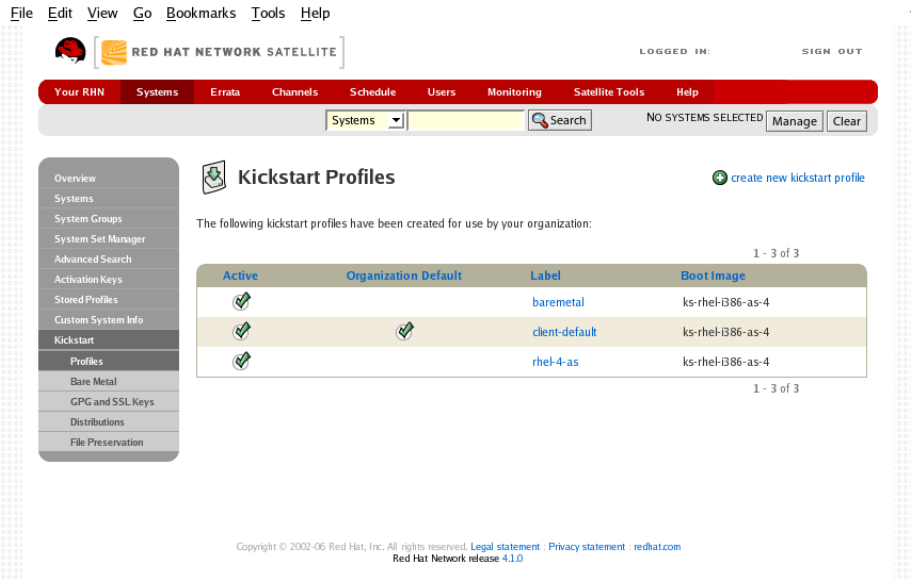


Figure 6.8. Kickstart Profiles

This page lists all profiles for your organization, whether those profiles are active, and the boot image to which that profile points. You can either create a new kickstart profile by clicking the **`create new kickstart profile`** link in the upper right or edit existing profiles by clicking in the name of the profile.

6.4.9.3. Create a New Kickstart Profile

If you are not using RHN Satellite, and wish to develop a new kickstart profile, first create a distribution through the **`Systems`** ⇒ **`Kickstart`** ⇒ **`Distributions`** page. Refer to Section 6.4.9.6, “Kickstart ⇒ Distributions — ” for instructions. Once that is done, return to the **`Kickstart Overview`** page to create the Kickstart Profile.

Click on the **`Create a New Kickstart Profile`** link from the **`Systems`** ⇒ **`Kickstart`** page to start the brief wizard that populates the base values needed for a kickstart profile.

1. On the first page, enter a kickstart profile label and select a kickstartable tree for this profile. The kickstartable tree drop-down menu is only populated if one or more distributions have been created for the selected base channel.
2. On the second page, select (or enter) the URL of the kickstart tree.
3. On the third page, select a root password for the system. Be sure to follow the password recommendations from the *Password Security* section of the *Red Hat Enterprise Linux Security Guide*, available at http://www.redhat.com/docs/manuals/enterprise/.

The final stage of the wizard presents the **`Kickstart Details`** ⇒ **`Details`** tab. On this tab and the other sub-tabs, nearly every option for the new kickstart profile can be customized. The following sections describe the options available on each sub-tab.

6.4.9.3.1. Kickstart Details ⇒ Details —

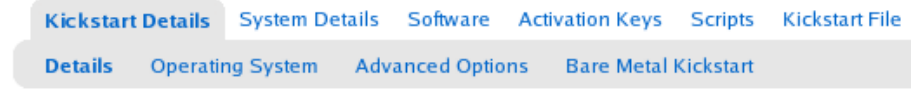


Figure 6.9. Kickstart Details

The figure above shows the sub-tabs that are available from the **Kickstart Details** tab.

From the **Kickstart Details** ⇒ **Details** sub-tab, you can:

- Rename the profile
- Change the operating system it installs by clicking (**Change**)
- Deactivate the profile so that it cannot be used to schedule a kickstart by removing the **Active** checkmark
- Select whether this profile is the default for all of your organization's kickstarts by checking or unchecking the box.
- Enter comments that are useful to you in distinguishing this profile from others

6.4.9.3.2. Kickstart Details ⇒ Operating System —

From this page, you can make the following changes to the operating system that the kickstart profile installs:

Change the base channel

Select from the available base channels, such as Red Hat Enterprise Linux AS version 4. Satellite customers see a list of all base channels that are currently synced to their Satellite.

File Location

The exact location from which the kickstart tree is mounted. This value is determined when the profile is created. You can view it on this page but you cannot change it.

6.4.9.3.3. Kickstart Details ⇒ Advanced Options —

From this page, you can toggle several installation options on and off by checking and unchecking the boxes to the left of the option. For most installations, the default options are correct. The *Red Hat Enterprise Linux System Administration Guide* discusses each of these options in detail.

6.4.9.3.4. Kickstart Details ⇒ Bare Metal Kickstart —

This sub-tab provides the information necessary to kickstart systems that are not currently registered with RHN. Using the on-screen instructions, you may either kickstart systems using boot media (CD-ROM) or by IP address.

6.4.9.3.5. System Details ⇒ Details —

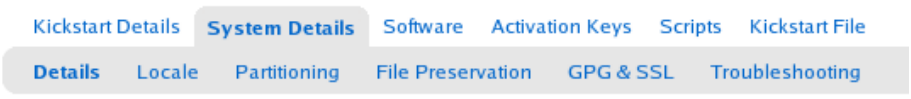


Figure 6.10. System Details

The figure above shows the sub-tabs that are available from the **System Details** tab.

From the **System Details** ⇒ **Details** sub-tab, you can:

- Select from DHCP and static IP, depending on your network
- Choose the level of SELinux that is configured on kickstarted systems
- Enable configuration management or remote command execution on kickstarted systems
- Change the root password associated with this profile

6.4.9.3.6. System Details ⇒ Locale —

From this sub-tab, you can change the timezone associated with kickstarted systems.

6.4.9.3.7. System Details ⇒ Partitioning —

From this sub-tab, you can indicate the partitions that you wish to be created during installation. For example:

```
 partition /boot --fstype=ext3 --size=200 partition swap --size=2000
partition pv.01 --size=1000 --grow volgroup myvg pv.01 logvol / --vgname=myvg
--name=rootvol --size=1000 --grow
```

6.4.9.3.8. System Details ⇒ File Preservation —

If you have previously created a file preservation list, you may include that list as part of the kickstart. This will prevent the files in that list from being over-written during the installation process. Refer to Section 6.4.9.7, “Kickstart ⇒ File Preservation —” for information on how to create a file preservation list.

6.4.9.3.9. System Details ⇒ GPG and SSL —

From this sub-tab, select the GPG keys and/or SSL certificates to be imported to the kickstarted system during the %post section of the kickstart. For Satellite customers, this list includes the SSL Certificate used during the installation of the Satellite.

Note

Any GPG key you wish to import to the kickstarted system must be in ASCII rather than binary format.

6.4.9.3.10. System Details ⇒ Troubleshooting —

From this sub-tab, you can change information that may help with troubleshooting hardware problems:

Bootloader

For some headless systems, it is better to select the non-graphic LILO bootloader.

Kernel Parameters

Enter kernel parameters here that may help to narrow down the source of hardware issues.

6.4.9.3.11. Software ⇒ Package Groups —

Figure 6.11. Software

The figure above shows the sub-tabs that are available from the **Software** tab.

Enter the package groups, such at **@office** or **@admin-tools** you would like to install on the kickstarted system in the large text box on this page. If you would like to know what package groups are available, and what packages they contain, refer to the **RedHat/base/** file of your kickstart tree. Satellite customers will most likely locate this file here: **/var/www/satellite/rhn/kickstart/<*kickstart label*>/RedHat/base/comps.xml**.

6.4.9.3.12. Software ⇒ Package Profiles —

If you have previously created a Package Profile from one of your registered systems, you can use that profile as a template for the files to be installed on a kickstarted system. Refer to Section 6.4.2.9.2.2, "System Details ⇒ Software ⇒ Packages" for more information about package profiles.

6.4.9.3.13. Activation Keys —

Figure 6.12. Activation Keys

The **Activation Keys** tab, which has no sub-tabs, allows you select Activation Keys to include as part of the kickstart profile. These keys, which must have been created previous to creating the kickstart profile, will be used when re-registering kickstarted systems.

6.4.9.3.14. Scripts —

Figure 6.13. Scripts

The **Scripts** tab, which has no sub-tabs, is where %pre and %post scripts are created. This page lists any scripts that have already been created for this kickstart profile. To create a new kickstart script:

1. Click the add new kickstart script link in the upper right
2. Enter the path to the scripting language used to create the script, such as /usr/bin/perl
3. Enter the full script in the large text box
4. Indicate whether this script is to be executed in the %pre or %post section of the kickstart process
5. Indicate whether this script is to run outside of the chroot environment. Refer to the *Post-installation Script* section of the *Red Hat Enterprise LinuxSystem Admin Guide* for further explanation of the **nochroot** option

Note

RHN supports the inclusion of separate files within the Partition Details section of the kickstart profile. For instance, you may dynamically generate a partition file based on the machine type and number of disks at kickstart time. This file can be created via %pre script and placed on the system, such as **/tmp/part-include**. Then you can call for that file by including the following line within the Partition Details field of the **System Details** ⇒ **Partitioning** tab:

```
%include /tmp/part-include
```

6.4.9.3.15. Kickstart File —

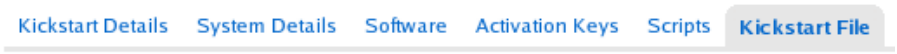


Figure 6.14. Kickstart File

The **Kickstart File** tab, which has no sub-tabs, allows you to view or download the kickstart profile that has been generated from the options chosen in the previous tabs.

6.4.9.4. Kickstart ⇒ Bare Metal —

Lists the IP addresses that have been associated with kickstart profiles created by your organization. Click either the range or the profile name to access different tabs of the **Kickstart Details** page.

6.4.9.5. Kickstart ⇒ GPG and SSL Keys —

Lists keys and certificates available for inclusion in kickstart profiles and provides a means to create new ones. This is especially important for customers of RHN Satellite or RHN Proxy Server because systems kickstarted by them must have the server key imported into RHN and associated with the relevant kickstart profiles. Import it by creating a new key here and then make the profile association in the **GPG and SSL keys** subtab of the **Kickstart Details** page.

To develop a new key/certificate, click the **create new stored key/cert** link in the upper-right corner of the page. Enter a description, select the type, upload the file, and click the **Update Key** button. Note that a unique description is required.

Important

The GPG key you upload to RHN must be in ASCII format. Using a GPG key in binary format causes anaconda, and therefore the kickstart process, to fail.

6.4.9.6. Kickstart ⇒ Distributions —

Enables you to identify custom installation trees that may be used for kickstarting. (Satellite users should note that this does not display Red Hat distributions provided to them. They can be found within the **Distribution** dropdown menu of the **Kickstart Details** page.) Before creating a distribution, you must make an installation tree available, as described in the *Kickstart Installations* chapter of the *Red Hat*

Enterprise Linux 4 System Administration Guide. This tree must be located in a public directory on an HTTP or FTP server.

Important

RHN Satellite users should note that channels imported with **satellite-sync** are made available automatically and do not require the creation of a separate installation tree. These trees are available to client systems that kickstart through the Satellite. While you may be able to access the files from a non-kickstarting client, this functionality is not supported and may be removed at any time in the future.

To create a new distribution, enter an intuitive label (without spaces) in the **Distribution Label** field, such as **my-orgs-rhel-as-4**. In the **External Location** field, paste the URL to the base of the installation tree. (You can test this by appending "README" to the URL in a Web browser, pressing **Enter**, and ensuring that the distribution's readme file appears.)

In the **Kickstart RPM** field, enter the auto-ks kernel image for the distribution. You can find all of the available packages by searching packages for "auto-kickstart". Identify the appropriate package based upon the distribution to be kickstarted. It should look something like, "auto-kickstart-ks-rhel-i386-as-4". Strip everything preceding the "ks" to derive the boot image. For instance, in the above example, you would enter "ks-rhel-i386-as-4" in the **Kickstart RPM** field.

Select the matching distribution from the **Base Channel** and **Installer Generation** dropdown menus, such as **Red Hat Enterprise Linux AS (v.4 for x86)** and **Red Hat Enterprise Linux 4**, respectively. When finished, click the **Create** button.

6.4.9.7. Kickstart ⇒ File Preservation —

Collects lists of files to be protected and re-deployed on systems during kickstart. For instance, if you have many custom configuration files located on a system to be kickstarted, enter them here as a list and associate that list with the kickstart profile to be used.

To use this feature, click the **create new file preservation list** link at the top and enter a relevant label and all files and directories to be preserved on the resulting page. Enter absolute paths to all files and directories. Then click **Create List**.

Important

Although file preservation is useful, it does have limitations. First, each list is limited to a total size of 1 MB. Further, special devices like **/dev/hda1** and **/dev/sda1** are not supported. Finally, only file and directory names may be entered. No regular expression wildcards can be included.

When finished, you may include the file preservation list in the kickstart profile to be used on systems containing those files. Refer to Section 6.4.9.3, “Create a New Kickstart Profile” for precise steps.

6.5. Errata

Select the **Errata** tab from the top navigation bar to track the availability and application of errata to your managed systems.

The first page to appear here is the **Errata Overview** page. This page displays relevant errata, which are errata that apply to at least one system to which you have administrative access and that have not yet been applied.

Tip

To receive an email when Errata Updates are issued for your system, go to **Your RHN** ⇒ **Your Preferences** and select **Receive email notifications**.

Red Hat releases Errata Updates in three categories, or types: Security Updates, Bug Fix Updates, and Enhancement Updates. Each Errata Update is comprised of a summary of the problem and the solution, including the RPM packages required to fix the problem.

Icons are used to identify the three types of Errata Updates:

- — Security Updates available, update *strongly* recommended
- — Bug Fix Updates available and recommended
- — Enhancement Updates available

A summary of each erratum is provided in list form. This view instantly informs you of the type, severity (for Security Updates), and subject of the erratum, as well as the number of affected systems.

In addition to the pages described within this chapter, you may view Errata by product line from the following location: https://rhn.redhat.com/errata.

6.5.1. Relevant Errata

As shown in Figure 6.15, “Errata List”, the **Relevant Errata** page displays a customized list of Errata Updates that applies to your registered systems. The list provides a summary of each Errata Update, including its type, severity (for Security Updates), advisory number, synopsis, systems affected, and date updated.

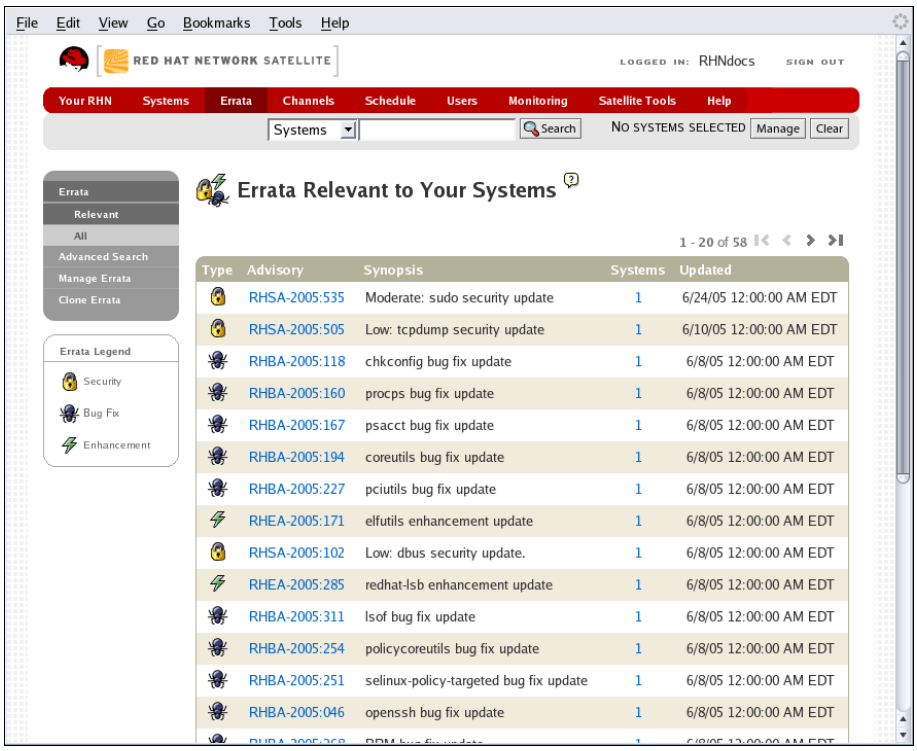

File Edit View Go Bookmarks Tools Help
RED HAT NETWORK SATELLITE
LOGGED IN: RHNdocs SIGN OUT
Your RHN Systems Errata Channels Schedule Users Monitoring Satellite Tools Help
Systems Search NO SYSTEMS SELECTED Manage Clear
Errata
Relevant
All
Advanced Search
Manage Errata
Clone Errata
Errata Legend
Security
Bug Fix
Enhancement
Errata Relevant to Your Systems
1 - 20 of 58
Type Advisory Synopsis Systems Updated
RHSA-2005:535 Moderate: sudo security update 1 6/24/05 12:00:00 AM EDT
RHSA-2005:505 Low: tcpdump security update 1 6/10/05 12:00:00 AM EDT
RHBA-2005:118 chkconfig bug fix update 1 6/8/05 12:00:00 AM EDT
RHBA-2005:160 procps bug fix update 1 6/8/05 12:00:00 AM EDT
RHBA-2005:167 psacct bug fix update 1 6/8/05 12:00:00 AM EDT
RHBA-2005:194 coreutils bug fix update 1 6/8/05 12:00:00 AM EDT
RHBA-2005:227 pciutils bug fix update 1 6/8/05 12:00:00 AM EDT
RHEA-2005:171 elfutils enhancement update 1 6/8/05 12:00:00 AM EDT
RHSA-2005:102 Low: dbus security update. 1 6/8/05 12:00:00 AM EDT
RHEA-2005:285 redhat-lsb enhancement update 1 6/8/05 12:00:00 AM EDT
RHBA-2005:311 lsof bug fix update 1 6/8/05 12:00:00 AM EDT
RHBA-2005:254 policycoreutils bug fix update 1 6/8/05 12:00:00 AM EDT
RHBA-2005:251 selinux-policy-targeted bug fix update 1 6/8/05 12:00:00 AM EDT
RHBA-2005:046 openssh bug fix update 1 6/8/05 12:00:00 AM EDT

Figure 6.15. Errata List

Clicking on the Advisory takes you to the **Details** tab of the **Errata Details** page. Clicking on the number of associated systems takes you to the **Affected Systems** tab of the **Errata Details** page. Refer to Section 6.5.2.2, “Errata Details” for more information.

6.5.2. All Errata

The **All Errata** page displays a list of all Errata Updates released by Red Hat. It works much the same as the **Relevant Errata** page in that clicking either the Advisory or the number of systems affected takes you to related tabs of the **Errata Details** page. Refer to Section 6.5.2.2, “Errata Details” for more information.

6.5.2.1. Apply Errata Updates

Errata Updates include a list of updated packages that are required to apply the Errata Update. To apply Errata Updates to a system, the system must be entitled.

Apply all applicable Errata Updates to a system by clicking on **Systems** ⇒ **Systems** in the top and left navigation bars. Click on the name of an entitled system, and click the **Errata** tab of the resulting **System Details** page. When the Relevant Errata list appears, click **Select All** then the **Apply Errata** button on the bottom right-hand corner of the page. Only those Errata that have not been scheduled or were scheduled and failed or canceled are listed. Updates already pending are excluded from the list.

In addition, Management users can apply Errata Updates using two other methods:

- To apply a specific Errata Update to one or more systems, find the update within the Errata lists. In the table, click on the number of systems affected, which takes you to the **Affected Systems** tab of the **Errata Details** page. Select the individual systems to be updated and click the **Apply Errata** button. Double-check the systems to be updated on the confirmation page, then click the **Confirm** button.

- To apply more than one Errata Update to one or more systems, select the systems from a **Systems** list and click the **Update List** button. Click the **System Set Manager** link in the left navigation bar, then click the **Systems** tab. After ensuring the appropriate systems are selected, click the **Errata** tab, select the Errata Updates to apply, and click the **Apply Errata** button. You can select to apply the Errata as soon as possible (the next time the Red Hat Network Daemon on the client systems connect to RHN) or schedule a date and time for the Errata Updates to occur. Then click the **Schedule Updates** button. You can follow the progress of the Errata Updates through the **Pending Actions** list. Refer to Section 6.7, “Schedule” for more details.

Important

If you use scheduled package installation, the packages are installed via the RHN Daemon. You must enable the RHN Daemon on your systems. Refer to Chapter 3, *Red Hat Network Daemon* for more details.

The following rules apply to Errata Updates:

- Each package is a member of one or more channels. If a selected system is not subscribed to a channel containing the package, the package will not be installed on that system.
- If a newer version of the package is already on the system, the package will not be installed on that system.
- If an older version of the package is installed, the package will be upgraded.

6.5.2.2. Errata Details

If you click on the Advisory of an Errata Update in the **Relevant** or **All** pages, its **Errata Details** page appears. This page is further divided into the following tabs:

6.5.2.2.1. Errata Details ⇒ Details

This subtab displays the Erratum Report issued by Red Hat. It provides a synopsis of the erratum first, including the severity (for security updates), issue date, and any update dates. This is followed by brief and detailed descriptions of the erratum and the steps required to resolve the issue.

Below the **Affected Channels** label, all channels that contain the affected package are listed. Clicking on a channel name displays the **Packages** subtab of the **Channel Details** page for that channel. Refer to Section 6.6.1.4, “Software Channel Details” for more information.

Below **Fixes**, the specific Bugzilla entries resolved by this erratum are listed. Clicking on any summary text opens that Bugzilla entry at http://bugzilla.redhat.com. Note that you must have a Bugzilla account to view the entry.

Security updates list the specific vulnerability as tracked by http://cve.mitre.org. This information is listed below the **CVEs** label.

Red Hat provides security update information in OVAL format. OVAL is an open vulnerability and assessment language promoted by Mitre, http://oval.mitre.org. Clicking on the link below the **Oval** label downloads this information to your system.

6.5.2.2.2. Errata Details ⇒ Packages

Provides links to each of the updated RPMs broken down by channel. Clicking on the name of a package

displays its **Package Details** page.

6.5.2.2.3. Errata Details ⇒ Affected Systems

Lists systems affected by the Errata Update. You can apply updates here. (See Section 6.5.2.1, “Apply Errata Updates”.) Clicking on the name of a system takes you to its **System Details** page. Refer to Section 6.4.2.9, “System Details” for more information.

To help users determine whether an update has been scheduled, a Status column exists within the affected systems table. Possible values are: None, Pending, Picked Up, Completed, and Failed. This column identifies only the latest action related to an Erratum. For instance, if an action fails and you reschedule it, this column shows the status of the Erratum as Pending (with no mention of the previous failure). Clicking a status other than None takes you to the **Action Details** page. This column corresponds to one on the **Errata** tab of the **System Details** page.

6.5.3. Advanced Search

The **Advanced Search** page allows you to search through Errata according to specific criteria, such as summary, advisory, and package name. Type a keyword, select the criterion to search by, and click the **Search** button. The results appear at the bottom of the page.

6.6. Channels

If you click the **Channels** tab on the top navigation bar, the **Channels** category and links appear. The pages in the **Channels** category enable you to view and manage the channels and packages associated with your systems. In addition, you can obtain ISO images here.

6.6.1. Software Channels

The **Software Channels** page is the first to appear in the **Channels** category. A software channel is a list of Red Hat Enterprise Linux packages grouped by use. Channels are used to choose packages to be installed on a system.

There are two types of software channels: *base channels* and *child channels*. A base channel consists of a list of packages based on a specific architecture and Red Hat Enterprise Linux release. For example, all of the packages in Red Hat Enterprise Linux 2.1 for the x86 architecture make up a base channel. The list of packages in Red Hat Enterprise Linux 2.1 for the Itanium architecture make up a different base channel. A child channel is a channel associated with a base channel that contains extra packages. For instance, an organization can create a child channel associated with Red Hat Enterprise Linux 2.1 for the x86 architecture that contains extra packages needed only for the organization, such as a custom engineering application.

A system must be subscribed to one base channel only. This base channel is assigned automatically during registration based upon the Red Hat Enterprise Linux release and system architecture selected. In the case of public free channels, the action will succeed. In the case of paid base channels, this action will fail if an associated entitlement doesn't exist.

A system can be subscribed to multiple child channels of its base channel. Only packages included in a system's subscribed channels can be installed or updated on that system. Further, RHN Satellite and RHN Proxy Server customers have channel management authority. This authority gives them the ability to create and manage their own custom channels. Refer to the *RHN Channel Management Guide* for details.

Channels can be further broken down by their relevance to your systems. Two such lists emerge:

Relevant and **All**.

6.6.1.1. Relevant Channels

As shown in Figure 6.16, “Relevant Channels”, the **Relevant Channels** page is shown by default when you click **Software Channels** in the left navigation bar. It displays a list of channels now associated with your systems. Links within this list go to different tabs of the **Software Channel Details** page. Clicking on a channel name takes you to the **Details** tab. Clicking on the number of packages takes you to the **Packages** tab. Clicking on the number of systems number takes you to the **Subscribed Systems** tab. Refer to Section 6.6.1.4, “Software Channel Details” for details.

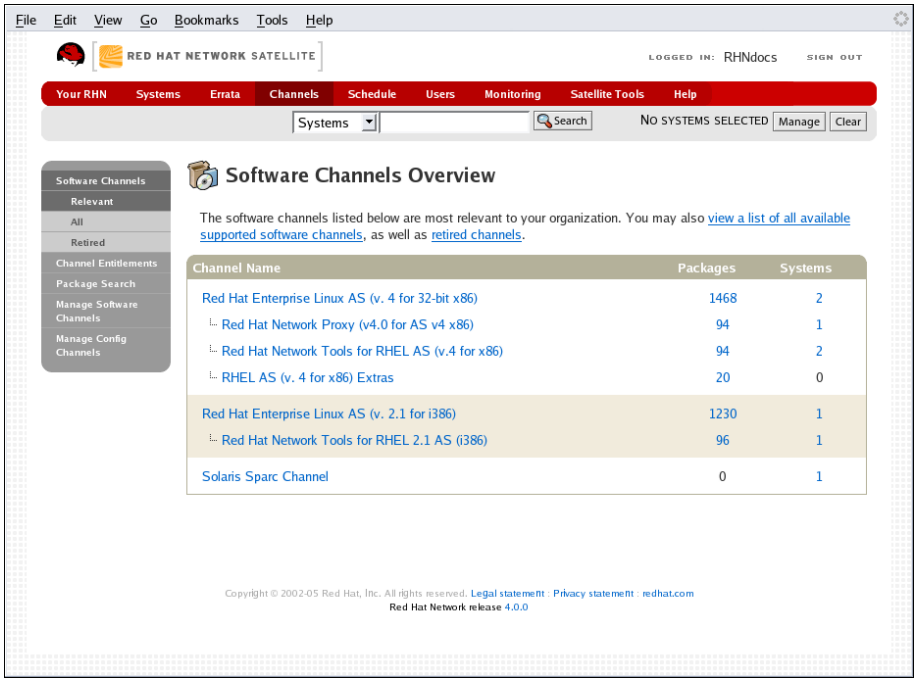


Figure 6.16. Relevant Channels

6.6.1.2. Retired Channels

The **Retired Channels** page displays channels available to your organization that have reached their end-of-life dates. These channels do not receive updates.

6.6.1.3. All Channels

The **All Channels** page can be retrieved by clicking **All** below **Software Channels** in the left navigation bar. It works identically to the **Relevant** button with one exception; it displays all software channels offered by Red Hat Network, regardless of whether you have systems associated with them.

6.6.1.4. Software Channel Details

If you click on the name of a channel, the **Software Channel Details** page appears. This page is broken down into the following tabs:

6.6.1.4.1. Software Channel Details ⇒ Details

General information about the channel and the parent channel, if it is a child channel. This is the first tab displayed when you click on a channel. It displays essential information about the channel, such as summary, description, and architecture.

—In addition, a Globally Subscribable checkbox can be seen by Organization Administrators and Channel Administrators. This signifies the default behavior of every channel allowing any user to subscribe systems to it. Unchecking this box and clicking **Update** causes the appearance of a **Subscribers** tab, which may then be used to grant certain users subscription permissions to the channel. Organization Administrators and Channel Administrators can always subscribe systems to any channel.

— Only customers with custom base channels may change their systems' base channel assignment. They may do this through the website in two ways:

- Customers with a custom base channel may assign the system to that base channel.
- Customers may revert system subscriptions from a custom base channel to the appropriate distribution-based base channel.

Note

The system base channel's distribution variant must match the variant installed on the system. For example, a system that has Red Hat Enterprise Linux AS v.4 for x86 cannot be registered to a Red Hat Enterprise Linux ES v.4 for x86 base channel.

6.6.1.4.2. Software Channel Details ⇒ Subscribers —

List of users who have subscription permissions to the channel. This tab appears on two conditions: First, the user must be an Organization Administrator or a Channel Administrator. Second, the Globally Subscribable checkbox on the **Details** tab must be unchecked, thereby making the channel subscribable by user. On this tab, select the checkboxes of the users to be allowed to subscribe systems to this channel and click **Update**. Note that Organization Administrators and Channel Administrators automatically have subscription access to all channels.

6.6.1.4.3. Software Channel Details ⇒ Managers —

List of users who have permission to manage the channel. This tab is applicable only to RHN Proxy Server and RHN Satellite customers with custom channel management privileges. It works much like the **Subscribers** tab but is available only for channels owned by the organization. There is no Globally Manageable flag like there is for subscription. A check in the **Managers** tab for a channel means that a user is a Channel Administrator for that channel alone. The user cannot create new channels or clone them.

6.6.1.4.4. Software Channel Details ⇒ Errata

List of Errata affecting the channel. The list displays advisory types, names, summaries, and the dates issued. Clicking on an advisory name takes you to its **Errata Details** page. Refer to Section 6.5.2.2, “Errata Details” for more information.

6.6.1.4.5. Software Channel Details ⇒ Packages

List of packages in the channel. To download packages as a .tar file, select them and click the **Download Packages** button at the bottom-left corner of the page. Clicking on a package name takes you to the **Package Details** page. This page displays a set of tabs with information about the package, including which architectures it runs on, the package size, build date, package dependencies, the change log, list of files in the package, newer versions, and which systems have the package installed. From here, you can download the packages as RPMs or SRPMs.

To search for a specific package or a subset of packages, use the package filter at the top of the list. Enter a substring to search all packages in the list for package names that contain the string. For example, typing **ks** in the filter might return: **ksconfig**, **krb5-workstation**, and **links**. The filter is case-insensitive.

6.6.1.4.6. Software Channel Details ⇒ Subscribed Systems

List of entitled systems subscribed to the channel. The list displays system names, base channels, and their levels of entitlement. Clicking on a system name takes you to its **System Details** page. Refer to Section 6.4.2.9, "System Details" for more information.

—If it is a child channel, you also have the option of unsubscribing systems from the channel. Use the checkboxes to select the systems, then click the **Unsubscribe** button on the bottom right-hand corner.

6.6.1.4.7. Software Channel Details ⇒ Target Systems

List of entitled systems that are eligible for subscription to the channel. This tab appears only for child channels. Use the checkboxes to select the systems, then click the **Subscribe** button on the bottom right-hand corner. You will receive a success message or be notified of any errors. This can also be accomplished through the **Channels** tab of the **System Details** page. Refer to Section 6.4.2.9, "System Details" for more information.

6.6.1.4.8. Software Channel Details ⇒ Downloads

ISO images associated with the channel. This tab appears only for base channels. Links on the **Easy ISOs** pages bring you to this tab for the related channel. Red Hat recommends using **curl** or **wget** for ISO downloads. Click the **help on using curl or wget** link for precise instructions.

6.6.1.4.9. Software Channel Details ⇒ License

Text of the channel's End User License Agreement. This tab is associated only with channels of third-party providers. It appears when you attempt to subscribe to such a channel through the **Target Systems** tab. To complete the subscription, read the agreement, click the **Accept** button, and then click the **Confirm** button. To decline the subscription, click the **Cancel** button.

6.6.2. Channel Entitlements

The **Channel Entitlements** page displays the list of channels for which you have paid. Click the number of systems subscribed to see a list of systems tied to the corresponding channel.

6.6.3. Download Software

The **Download Software** pages provide direct access to the ISO images available to you. These images, comprising full installations of various Red Hat operating system distributions, are actually located within the **Downloads** tab of the **Channel Details** page. This feature is available only to paid RHN subscribers.

To download an ISO image, Red Hat recommends copying its URL and using either **curl** or **wget**. Click the **help on using curl or wget** link for precise instructions. To obtain the URL, right-click on the disc link and choose to open the link in a new window or tab. You may then cancel the download, copy the lengthy URL from the location bar, and paste it into the **curl** or **wget** command.

Once downloaded, either burn the images to CD-Rs or CD-RWs or copy them to the machine for direct installation. Refer to http://www.redhat.com/download/howto_download.html for additional download

instructions and steps to burn images to discs. Refer to the operating system's respective installation guide for instructions on installing from CD-ROM or hard drive, available at http://www.redhat.com/docs/.

ISOs can be further broken down by their relevance to your systems. Two such lists emerge: **Relevant** and **All**.

6.6.3.1. Relevant ISOs

The **Relevant ISOs** page is shown by default when you click **Download Software** in the left navigation bar. It displays a list of ISOs by channel now associated with your systems. Links within this list go to the **Downloads** tab of the **Channel Details** page. Refer to Section 6.6.3, “Download Software” for instructions on use.

6.6.3.2. All ISOs

The **All ISOs** page can be retrieved by clicking **All** below **Easy ISOs** in the left navigation bar. It works identically to the **Relevant** button with one exception; It displays all ISOs available to you through Red Hat Network, regardless of whether you have systems associated with the related channels. Refer to Section 6.6.3, “Download Software” for instructions on use.

6.6.4. Package Search

The **Package Search** page allows you to search through packages using various criteria. You may search by name or name and summary, within relevant or all channels, or within specific architectures. Type a keyword, select the criterion by which to search, and click the **Search** button. The results appear at the bottom of the page.

6.6.5. Manage Software Channels

This tab allows Administrators to create, clone, and delete custom channels. These channels may contain altered versions of distribution-based channels or custom packages.

6.6.5.1. Manage Software Channels ⇒ Channel Details

The default screen of the Manage Software Channels tab is a listing of all available channels. This includes custom, distribution-based, and child channels.

To clone an existing channel, click the **clone channels** link in the upper right of the screen, select the channel to be cloned from the dropdown menu, and click the **Create Channel** button. The next screen presents various options for the new channel, including base architecture and GPG options. Make your selections and click the **Create Channel** button to complete the process.

To create a new channel, click the **create new channel** link in the upper right of the screen. Select the various options for the new channel, including base architecture and GPG options. Make your selections and click the **Create Channel** button. Note that a channel created in this manner is blank, containing no packages. You must either upload software packages or add packages from other channels. You may also choose to include Errata Updates in your custom channel.

6.6.5.1.1. Manage Software Channels ⇒ Channel Details ⇒ Channel Details

This screen lists the selections you made during the channel creation process. This page includes the **Globally Subscribable** checkbox that permits all users to subscribe to the channel.

6.6.5.1.2. Manage Software Channels ⇒ Channel Details ⇒ Managers

This subtab allows you to select which users may alter or delete this channel. Organization Administrators and Channel Administrators may alter or delete any channel.

To allow a user to alter the channel, select the checkbox next to the user's name and click the **Update** button. To allow all users to manage the channel, click the **Select All** button at the bottom of the list followed by the **Update** button. To remove a user's ability to manage the channel, uncheck the box next to their name and click the **Update** button.

6.6.5.1.3. Manage Software Channels ⇒ Channel Details ⇒ Errata

This subtab allows channel managers to list, remove, clone, and add Errata to their custom channel. Custom channels not cloned from a distribution may not add Errata until there are packages in the channel. Only Errata that match the base architecture of the channel and apply to a package in that channel may be added to the channel. Finally, only cloned or custom Errata may be added to custom channels. Errata may be included in a cloned channel if they are selected during channel creation.

6.6.5.1.4. Manage Software Channels ⇒ Channel Details ⇒ Packages

This subtab is similar to the Errata subtab. It allows Channel and Organization Administrators to list, remove, compare, and add packages to the custom channel.

To list all packages in the channel, click the **List / Remove Packages** link. Check the box to the left of any package you wish to remove, then click the **Remove Packages** button in the lower right of the page.

To add packages, click the **Add Packages** link. Choose a channel from which to select packages from the drop-down menu and click the **View** button to continue. Check the box to the left of any package you wish to add to the channel, then click the **Add Packages** button in the bottom right of the screen.

To compare packages within the current channel with those of another channel, select the other channel from the drop-down menu and click the **Compare** button. All packages present in either channel are compared, and the results displayed on the next screen. This information includes the architecture and version of each package.

To make the two channels identical, click the **Merge Differences** button in the lower right. The following screen allows you to select how conflicts are resolved. Click the **Preview Merge** button to view the results of the merging without making any changes to the channels. Finally, select those packages that you wish to merge and click the **Merge Packages** button followed by the **Confirm** button to perform the merge.

6.6.5.2. Manage Software Channels ⇒ Manage Software Packages

This tab allows you to manage custom software packages owned by your organization. You may view a list of all custom software or view only those packages in a selected custom channel. To select the channel whose custom packages you wish to view, select the channel from the drop-down menu and click the **View** button.

6.6.6. Manage Config Channels —

Provides the means to create and oversee channels containing configuration files. You must be a Configuration Administrator or Organization Administrator to view this section of the website. Like software channels, configuration channels store files to be installed on systems. Unlike software packages, various versions of configuration files may prove useful to a system at any given time. Further, RHN allows you to include variables, or macros, that allow you to treat your configuration files as templates that can be deployed across your organization, with the relevant values populated upon individual system installation.

Please note that whenever a configuration file is deployed via RHN, a backup of the previous file including its full path is made in the **/var/lib/rhncfg/backups/** directory on the affected system. The backup retains its filename but has a **.rhn-cfg-backup** extension appended.

6.6.6.1. Preparing Systems for Config Management

For a system to have its configuration managed through RHN, it must have the appropriate tools and **config-enable** file installed. These tools may already be installed on your system, especially if you kickstarted the system with configuration management functionality. If not, they can be found within the RHN Tools child channel for your distribution. Download and install the latest **rhncfg*** packages. They are:

- **rhncfg** — The base libraries and functions needed by all **rhncfg-*** packages.
- **rhncfg-actions** — The code required to run configuration actions scheduled via the RHN website.
- **rhncfg-client** — A command line interface to the client features of the RHN Configuration Management system.
- **rhncfg-management** — A command line interface used to manage RHN configuration.

Next, you must enable your system to schedule configuration actions. This is done using the **rhn-actions-control** command on the client system. This command is included in the **rhncfg-actions** RPM. The RHN Actions Control (**rhn-actions-control**) enables or disables specific modes of allowable actions. Refer to Section A.1, "**Red Hat Network Actions Control**" for instructions.

6.6.6.2. Manage Config Channels ⇒ Config Channels —

There are two types of configuration channels: *global channels* and *system-specific channels*. A global channel contains configuration files developed across your organization. These may well be applicable to multiple systems. A system-specific channel consists of local override configuration files tied to particular systems. These files take precedent over all other configurations.

6.6.6.2.1. Manage Config Channels ⇒ Config Channels ⇒ Global —

Shown by default when you click **Manage Config Channels** in the left navigation bar, the **Global Config Channels** displays a list of configuration channels managed by your organization. Links within this list go to different tabs of the **Configuration Channel Details** page. Clicking on a channel name takes you to the **Details** tab. Clicking on the number of files takes you to the **Files** tab. Clicking on the number of systems takes you to the **Systems** tab. Refer to Section 6.6.6.5, "Configuration Channel Details — " for instructions.

6.6.6.2.2. Manage Config Channels ⇒ Config Channels ⇒ System —

The **System Config Channels** page can be retrieved by selecting it from the pulldown menu on the main **Manage Config Channels** page. It displays local override (system-specific) configuration channels and works similarly to the **Global Config Channels** page in that clicking the name of a system takes you to the **List** subtab of the **Configuration Channel Details** page. Refer to Section 6.6.6.5, "Configuration Channel Details — " for instructions.

6.6.6.3. Manage Config Channels ⇒ Manage Files —

The **Manage Files** page lists the configuration files managed by your organization. The files here are listed by path. A given path can exist in many configuration channels, but each instance of a path in each

configuration channel is treated as a separate entity.

Clicking the number in the Config Channels column takes you to a list of channels containing the file. From there you can access tabs of the **Configuration Channel Details** page. Clicking the number in the Latest Revision column takes you to the **Configuration File Details** page. Refer to Section 6.6.6.6, "Configuration File Details —" for instructions.

6.6.6.4. Manage Config Channels ⇒ Quota —

The **Quota** page displays the amount of disk space alloted and used for storing configuration files. A summary of available and used space can be found at the top, while individual file use is listed within the table. Click the file name to go to the **Configuration File Details** page. Refer to Section 6.6.6.6, "Configuration File Details —" for instructions. Click the config channel name to access the **Configuration Channel Details** page. Refer to Section 6.6.6.5, "Configuration Channel Details —" for instructions.

6.6.6.5. Configuration Channel Details —

If you click on the name of a channel in a list, the **Configuration Channel Details** page will appear. This page contains the following tabs:

6.6.6.5.1. Configuration Channel Details ⇒ Details —

General information about the channel. This is the first tab you see when you click on a channel. It displays basic information about the channel, including name and description, and provides the means to alter this information. To make changes, enter new values in the text fields and click the **Edit Config Channel** button.

6.6.6.5.2. Configuration Channel Details ⇒ Files —

Configuration files associated with this channel. Use the subtabs to view, upload, and create files.

6.6.6.5.2.1. Configuration Channel Details ⇒ Files ⇒ List —

Displays the files and directories associated with the configuration channel. Files are represented by a *paper* icon while directories display *folder* icons. Click the name of a file or directory to go to its details page. Refer to Section 6.6.6.6, "Configuration File Details —" for instructions. To replicate a file within a config channel, select its checkbox, click the **Copy to Config Channel** button, and select the destination channel. To remove a file, select it and click **Delete Selected Files**.

6.6.6.5.2.2. Configuration Channel Details ⇒ Files ⇒ Upload —

Enables you to import files from your system into RHN's central configuration manager. The Deploy File Path is the path to which the file will be deployed on a target system, and Local File is the file you want to upload from your system to RHN.

To upload a file, populate all fields, browse for the file, and click the **Upload File** button. Note that files larger than 16 KB cannot be edited through the RHN website. The file path is the location to which the file will be deployed. The user, group, and mode fields allow you to set the file's ownership and permissions.

6.6.6.5.2.3. Configuration Channel Details ⇒ Files ⇒ Create File —

Allows you to create a configuration file from scratch within the interface. The fields here work similarly to those on the **Upload** subtab: **Path** is the location to which the file will be deployed. The user, group, and mode fields allow you to set the file's ownership and permissions. Include the file contents in the **Contents** field. When finished, click the **Create Config File** button.

Note

You must enter a valid user and group for the system to which the file (or directory) will be deployed. If either is not valid, the deployment of the file fails with an error message similar to the following:

```
Error: unable to deploy file /root/example-config-file, information on
user 'jdoe' \ could not be found.
```

6.6.6.5.2.4. Configuration Channel Details ⇒ Files ⇒ Create Directory —

Allows you to create a configuration directory within the interface. The fields resemble those on the **Upload** and **Create File** subtab: Path is the absolute location of the directory on the system. The user, group, and mode fields allow you to set the directory's ownership and permissions. When finished, click the **Create Config Directory** button. Note that the user and group must be valid.

6.6.6.5.3. Configuration Channel Details ⇒ Systems —

Identifies the systems subscribed to this configuration channel. Clicking a system name takes you to the **System Details** page.

6.6.6.5.4. Configuration Channel Details ⇒ Target Systems —

Displays all of the systems that have Provisioning entitlements but are not yet subscribed to this config channel. To associate systems with the config channel, select their checkboxes and click the button matching the rank to be assigned. **Subscribe with Highest Rank** overrides all other config channels, except local configs. **Subscribe with Lowest Rank** ranks this config channel below all others. When done, the selected systems will appear in the **Systems** tab.

6.6.6.6. Configuration File Details —

If you click on the name or number of a file in a list, the **Configuration File Details** page will appear. You may remove the file at anytime by clicking **delete file** in the upper-right corner of the page. This page contains the following tabs:

6.6.6.6.1. Configuration File Details ⇒ Details —

General information about the file. This is the first tab you see when you click on a file. It displays basic information about the file, including path, associated channel, revision, and date. It also provides links to download, view and edit the file, and to identify whether it is binary. Note that files larger than 16 KB cannot be edited through the RHN website. In addition, you can define macros (variables) here that will have different values interpolated when installed on various systems. Refer to Section 6.6.6.7, “Including Macros in your Configuration Files” for a full description of this feature.

6.6.6.6.2. Configuration File Details ⇒ Revisions —

A list of the revisions of this configuration file in the current config channel. Every change to a configuration file creates a new revision of that file in the given config channel. The latest revision of a configuration file is always the only one provided by that channel. Revision numbers for a file are tied to a channel. So revision 3 of **/etc/example1** in config channel "config1" is completely independent of revision 3 of **/etc/example1** in config channel "config2". You can examine revisions in the list or use the **Browse** and **Upload File** buttons to upload a more recent revision.

6.6.6.6.3. Configuration File Details ⇒ Diff —

A list of configuration files available for comparison. Click the name of the channel containing the file, then the name of the file itself. A list of differences will appear.

6.6.6.6.4. Configuration File Details ⇒ Copy —

A list of configuration channels that may receive a copy of the file. To copy the file to a channel, select the channel's checkbox and click the **Copy File** button.

- **Copy to Config Channel** — Displays the global config channels for your organization. To copy the latest revision of this file to channels, select the appropriate checkboxes, and click the **Copy File** button.
- **Copy to System** — Displays the system-specific config channels for your organization. To copy the latest revision of this file to channels, select the appropriate checkboxes, and click the **Copy File** button.

6.6.6.7. Including Macros in your Configuration Files

Being able to store and share identical configurations is useful, but what if you have many variations of the same configuration file? What do you do if you have configuration files that differ only in system-specific details, such as hostname and MAC address?

In traditional file management, you would be required to upload and distribute each file separately, even if the distinction is nominal and the number of variations is in the hundreds or thousands. RHN addresses this by allowing the inclusion of macros, or variables, within the configuration files it manages for Provisioning-entitled systems. In addition to variables for custom system information, the following standard macros are supported:

- rhn.system.sid
- rhn.system.profile_name
- rhn.system.description
- rhn.system.hostname
- rhn.system.ip_address
- rhn.system.custom_info(key_name)
- rhn.system.net_interface.ip_address(eth_device)
- rhn.system.net_interface.netmask(eth_device)
- rhn.system.net_interface.broadcast(eth_device)
- rhn.system.net_interface.hardware_address(eth_device)
- rhn.system.net_interface.driver_module(eth_device)

To use this powerful feature, either upload or create a configuration file through the **Configuration Channel Details** page. Then, open its **Configuration File Details** page and include the supported macros of your choosing. Ensure that the delimiters used to offset your variables match those

set in the **Macro Start Delimiter** and **Macro End Delimiter** fields and do not conflict with other characters in the file. The delimiters must be two characters in length and cannot contain the percent (%) symbol.

As an example, you may have a file applicable to all of your servers that differs only in IP address and hostname. Rather than manage a separate configuration file for each server, you may create a single file, such as **server.conf**, with the IP address and hostname macros included, like so:

```
  hostname={@ rhn.system.hostname @} ip_address={@
rhn.system.net_interface.ip_address(eth0) @}
```

Upon delivery of the file to individual systems, whether through a scheduled action in the RHN website or at the command line with the **Red Hat Network Configuration Client** (**rhncfg-client**), the variables will be replaced with the hostname and IP address of the system, as recorded in RHN's System Profile. In the above configuration file, for example, the deployed version resembles the following:

```
hostname=test.example.domain.com ip_address=177.18.54.7
```

To capture custom system information, insert the key label into the custom information macro (rhn.system.custom_info). For instance, if you developed a key labeled "asset" you can add it to the custom information macro in a configuration file to have the value substituted on any system containing it. The macro would look like this:

```
asset={@ rhn.system.custom_info(asset) @}
```

Upon deployment of the file to a system containing a value for that key, the macro gets translated, resulting in a string similar to the following:

```
asset=Example#456
```

To include a default value, for instance if one is required to prevent errors, you can append it to the custom information macro, like so:

```
asset={@ rhn.system.custom_info(asset) = 'Asset #' @}
```

This default is overridden by the value on any system containing it. For instructions on developing custom system information keys, refer to Section 6.4.8, “Custom System Info — ”.

Using the **Red Hat Network Configuration Manager** (**rhncfg-manager**) will not translate or alter files, as that tool is system agnostic — **rhncfg-manager** does not depend on system settings. Binary files cannot be interpolated.

6.7. Schedule

If you click the **Schedule** tab on the top navigation bar, the **Schedule** category and links appear. These pages enable you to track the actions taking place within your systems. An action is a scheduled RHN task that is to be performed on one or more client systems. For example, an action can be scheduled to apply all Errata Updates to a system.

Red Hat Network keeps track of the following action types:

1. Package Alteration (installation, upgrade, and removal)

2. Rollback Package Actions
3. System Reboots
4. Errata Updates
5. Configuration File Alteration (deploy, upload, and diff)
6. Hardware Profile Updates
7. Package List Profile Updates
8. Kickstart Initiation
9. Remote Commands

Each page in the **Schedule** category represents an action status.

6.7.1. Pending Actions

As shown in Figure 6.17, “Schedule - Pending Actions”, the **Pending Actions** page is shown by default when you click **Schedule** in the top navigation bar. It displays actions that have not started or are in progress.

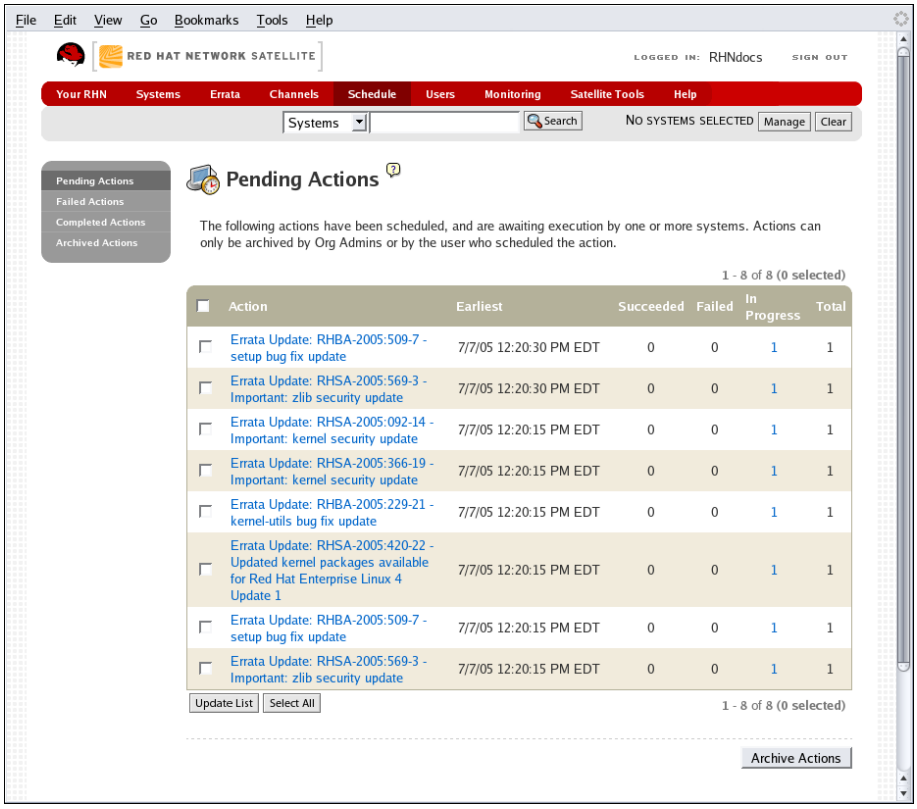

File Edit View Go Bookmarks Tools Help
RED HAT NETWORK SATELLITE
LOGGED IN: RHNdocs
SIGN OUT
Your RHN
Systems
Errata
Channels
Schedule
Users
Monitoring
Satellite Tools
Help
Systems
Search
NO SYSTEMS SELECTED
Manage
Clear
Pending Actions
Failed Actions
Completed Actions
Archived Actions
Pending Actions
The following actions have been scheduled, and are awaiting execution by one or more systems. Actions can only be archived by Org Admins or by the user who scheduled the action.
1 - 8 of 8 (0 selected)
Action
Earliest
Succeeded
Failed
In Progress
Total
Errata Update: RHBA-2005:509-7 - setup bug fix update
7/7/05 12:20:30 PM EDT
Errata Update: RHSA-2005:569-3 - Important: zlib security update
7/7/05 12:20:30 PM EDT
Errata Update: RHSA-2005:092-14 - Important: kernel security update
7/7/05 12:20:15 PM EDT
Errata Update: RHSA-2005:366-19 - Important: kernel security update
7/7/05 12:20:15 PM EDT
Errata Update: RHBA-2005:229-21 - kernel-utils bug fix update
7/7/05 12:20:15 PM EDT
Errata Update: RHSA-2005:420-22 - Updated kernel packages available for Red Hat Enterprise Linux 4 Update 1
7/7/05 12:20:15 PM EDT
Errata Update: RHBA-2005:509-7 - setup bug fix update
7/7/05 12:20:15 PM EDT
Errata Update: RHSA-2005:569-3 - Important: zlib security update
7/7/05 12:20:15 PM EDT
Update List
Select All
1 - 8 of 8 (0 selected)
Archive Actions

Figure 6.17. Schedule - Pending Actions

6.7.2. Failed Actions

Actions that could not be completed. If the action returns an error, it is displayed here.

6.7.3. Completed Actions

Actions that have succeeded.

6.7.4. Archived Actions

Actions that you have selected to store for review.

6.7.5. Actions List

In each page, each row in the list represents a single scheduled event or action that might affect multiple systems and involve various packages. The list contains several columns of information:

- **Select** — Use the checkboxes in this column to select actions. After selecting actions, you can either add them to your selection list or move them to the **Archived Actions** list. If you archive a pending action, it is not canceled; the action item moves from the **Pending Actions** list to the **Archived Actions** list.
- **Action** — Type of action to perform such as Errata Update or Package Install. Clicking an action name takes you to its **Action Details** page. Refer to Section 6.7.5.1, “Action Details” for more information.
- **Earliest** — The earliest day and time the action will be performed.
- **Succeeded** — Number of systems on which this action was successful.
- **Failed** — Number of systems on which this action has been tried and failed.
- **In Progress** — Number of systems on which this action is taking place.
- **Total** — Total number of systems on which this action has been scheduled.

6.7.5.1. Action Details

If you click on the name of an action, the **Action Details** page appears. This page is broken down into the following tabs:

6.7.5.1.1. Action Details ⇒ Details

General information about the action. This is the first tab you see when you click on an action. It displays the action type, scheduling administrator, earliest execution, and notes. Clicking the Errata Advisory takes you to the **Errata Details** page.The Errata Advisory appears only if the action is an Errata Update. Refer to Section 6.5.2.2, “Errata Details” for more information.

6.7.5.1.2. Action Details ⇒ Completed Systems

List of systems on which the action has been successfully undertaken. Clicking a system name takes you to its **System Details** page. Refer to Section 6.4.2.9, “System Details” for more information.

6.7.5.1.3. Action Details ⇒ In Progress Systems

List of systems on which the action is now being undertaken. To cancel an action, select the system using the appropriate checkbox and click the **Unschedule Action** button. Clicking a system name takes you to its **System Details** page. Refer to Section 6.4.2.9, “System Details” for more information.

6.7.5.1.4. Action Details ⇒ Failed Systems

List of systems on which the action has been attempted and failed. The actions can be rescheduled here. Clicking a system name takes you to its **System Details** page. Refer to Section 6.4.2.9, “System Details” for more information.

6.8. Users —

Only Organization Administrators can see the **Users** tab on the top navigation bar. If you click the **Users** tab, the **Users** category and links appear. These pages enable you to grant and edit

permissions for those who administer your system groups. Click in the **User List** to modify users within your organization.

To add new users to your organization, click the **create new user** link on the to right corner of the page. The next page is the **Create User** page. Fill in each of the required values for the new user.

Note

It is important that the email field is accurate, because the new user must respond to an email sent to that address before they will be able to login to RHN.

Once all fields are complete, select the **Create Login** button. RHN now sends an email to the specified address and redirects you to the **Users** ⇒ **User List** page. If you wish to select permissions and options for the newly created user, select their name from the list. Doing so displays the **User Details** page for that user, which provides several subtabs of options from which to choose. Refer to Section 6.8.1.1, "User List ⇒ Active ⇒ User Details — " for detailed descriptions of each subtab.

6.8.1. User List ⇒ Active —

This tab lists all active users of your RHN account. It displays the following basic information about each user: their username, real name, roles, and the date of their last sign in.

As shown in Figure 6.18, "User List", each row in the **User List** represents a user within your organization. There are four columns of information for each user:

- **Username** — The login name of the user. If you click on a username, the **User Details** page for the user is displayed. Refer to Section 6.8.1.1, "User List ⇒ Active ⇒ User Details — " for more information.
- **Real Name** — The full name of the user (last name first).
- **Roles** — List of the user's privileges, such as Organization Administrator, Channel Administrator and normal user. Users can have multiple roles.
- **Last Sign In** — Shows when the user last logged into RHN.

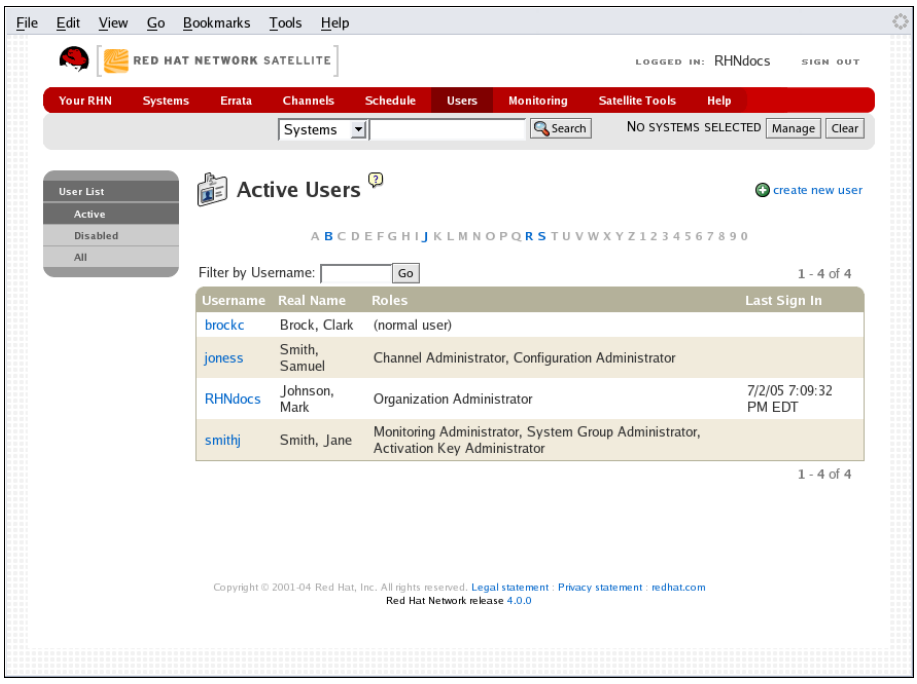

File Edit View Go Bookmarks Tools Help
RED HAT NETWORK SATELLITE
LOGGED IN: RHNdocs SIGN OUT
Your RHN Systems Errata Channels Schedule Users Monitoring Satellite Tools Help
Systems Search NO SYSTEMS SELECTED Manage Clear
User List
Active
Disabled
All
Active Users
create new user
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 1 2 3 4 5 6 7 8 9 0
Filter by Username: Go
1 - 4 of 4
Username Real Name Roles Last Sign In
brockc Brock, Clark (normal user)
joness Smith, Samuel Channel Administrator, Configuration Administrator
RHNdocs Johnson, Mark Organization Administrator 7/2/05 7:09:32 PM EDT
smithj Smith, Jane Monitoring Administrator, System Group Administrator, Activation Key Administrator
1 - 4 of 4
Copyright © 2001-04 Red Hat, Inc. All rights reserved. Legal statement | Privacy statement | redhat.com
Red Hat Network release 4.0.0

Figure 6.18. User List

6.8.1.1. User List ⇒ Active ⇒ User Details —

The **`User Details`** page allows Organization Administrators to manage the permissions and activity of all users. Included in the **`User Details`** page is the ability to delete or deactivate users.

Users may now be deactivated directly from the RHN web interface. RHN Satellite customers may deactivate or delete users from their systems, although non-Satellite customers must contact Customer Service to delete a user. Users may be deactivated or deleted by Organization Administrators, or users may deactivate their own accounts.

Deactivated users cannot log in to the RHN web interface, nor may they schedule any actions. Organization Administrators may not be deactivated until that role is removed from their account. Actions scheduled by a user prior to their deactivation remain in the action queue. For added flexibility, deactivated users may be reactivated by Organization Administrators.

User deletion from the web interface is available exclusively to RHN Satellite customers. The Organization Administrator role must be removed from a user before that individual may be deleted.

Warning

User deletion is irreversible; exercise it with caution. Consider disabling the user first in order to assess the effect deletion will have on your infrastructure.

To deactivate a user:

1. Navigate to the user's **`User Details`** tab.
2. Verify that the user is not an Organization Administrator. If they are, uncheck the box to the left of that role and click the **`Submit`** button in the lower right of the screen.

3. Click the **deactivate user** link in the upper right of the screen.
4. Click the **Deactivate User** button in the lower right to confirm.

To delete a user:

1. Navigate to the user's **User Details** tab.
2. Verify that the user is not an Organization Administrator and remove that role if necessary.
3. Click the **delete user** link in the upper right.
4. Click the **Delete User** button to permanently delete the user.

For instructions regarding deactivating your own account, refer to Section 6.3.1.3, “Account Deactivation”.

6.8.1.1.1. User List ⇒ Active ⇒ User Details ⇒ Details —

This is the default **User Details** tab, which displays the username, first name, last name, email address, and user roles for the user. All of this information is modifiable. To do so, make your changes and click the **Update** button. Remember, when changing a user's password, you will see only asterisks as you type the password.

To delegate responsibilities within your organization, Red Hat Network provides several roles with varying degrees of responsibility and access. This list describes the permissions of each and the differences between them:

- **User** — Also known as a *System Group User*, this is the standard role associated with any newly created user. This person may be granted access to manage system groups and software channels. The systems must be in system groups to which the user has permissions for them to be manageable or even visible. Remember, however, all globally subscribable channels may be used by anyone.
- **Activation Key Administrator** — This role is designed to manage your organization's collection of activation keys. This person can create, modify, and delete any key within your overarching account.
- **certificate authority** — This role has complete access to the software channels and related associations within your organization. It requires RHN Satellite or RHN Proxy Server. This person may change the base channels of systems, make channels globally subscribable, and create entirely new channels.
- **Configuration Administrator** — This role enables the user to manage the configuration of systems in the organization using either the RHN website or the **Red Hat Network Configuration Manager**.
- **Monitoring Administrator** — This role allows for the scheduling of probes and oversight of other Monitoring infrastructure. This role is available only on Monitoring-enabled RHN Satellite version 3.6 or later.
- **Organization Administrator** — This role can perform any function available within Red Hat Network. As the master account for your organization, the person holding this role can alter the privileges of all other accounts, as well as conduct any of the tasks available to the other roles. Like the other roles, multiple Organization Administrators may exist.
- **System Group Administrator** — This role is one step below Organization Administrator in that it has complete authority over the systems and system groups to which it is granted access. This person can create new system groups, delete any assigned systems groups, add systems to groups, and manage user access to groups.

While it is possible for one Organization Administrator to remove Organization Administrator rights from

another user, it is impossible to remove Organization Administrator rights from the sole remaining Organization Administrator. It is possible to remove your own Organization Administrator privileges so long as you are not the last Organization Administrator.

To assign a user a new role, select the appropriate checkbox. Remember that Organization Administrators are automatically granted administration access to all other roles, signified by grayed-out checkboxes. To grant a user the ability to manage the configuration of systems, select the **Configuration Administrator** checkbox. When satisfied with the changes, click **Update**.

6.8.1.1.2. User List ⇒ Active ⇒ User Details ⇒ System Groups —

This tab displays a list of system groups that the user may administer. Organization Administrators may use the check boxes to set this user's access permissions to each system group. Check or uncheck the box to the left of the system group and click the **Update Permissions** button to save the changes.

Organization Administrators may select one or more default system groups for this user. When the user registers a system, that system is assigned to the selected group or groups. This allows the user to have access to the newly-registered system immediately, if he or she has permissions to one or more of the groups to which the system is assigned. System Groups to which this user has access are preceded by an (*).

6.8.1.1.3. User List ⇒ Active ⇒ User Details ⇒ Systems —

This tab lists all systems to which the user has access permission. These systems come from the system groups assigned to the user on the previous tab. You may choose a set of systems to work with by checking the boxes to the left of the systems and clicking the **Update List** button. Use the System Set Manager page to execute actions on those systems. Clicking the name of a system takes you to its **System Details** page. Refer to Section 6.4.2.9, “System Details” for more information.

6.8.1.1.4. User List ⇒ Active ⇒ User Details ⇒ Channel Permissions —

This tab lists all channels available to your organization. You may grant explicit channel subscription permission to this user for each of the channels listed by checking the box to the left of the channel and clicking the **Update Permissions** button. Permissions granted through Organization Administrator status, certificate authority status, or because the channel is globally subscribable have no checkbox, but display a check icon instead.

6.8.1.1.4.1. User List ⇒ Active ⇒ User Details ⇒ Channel Permissions ⇒ Subscription —

Identifies channels to which the user may subscribe systems. To change these, select or unselect the appropriate checkboxes and click the **Update Permissions** button. Note that channels subscribable through the user's admin status or the channel's global setting cannot be altered. They are identified with a check icon.

6.8.1.1.4.2. User List ⇒ Active ⇒ User Details ⇒ Channel Permissions ⇒ Management —

Identifies channels the user may manage. To change these, select or unselect the appropriate checkboxes and click the **Update Permissions** button. This status does not enable the user to create new channels. Note that channels automatically manageable through the user's admin status cannot be altered. They are identified with a check icon. Remember, Organization Administrators and Channel Administrators can subscribe to or manage any channel.

6.8.1.1.5. User List ⇒ Active ⇒ User Details ⇒ Preferences —

This page allows you to configure whether the user receives email notifications, the number of entries displayed per list page, and the timezone of the user. Make selections and click the **Save Preferences** button to update.

- Email Notification — Determine whether this user should receive email every time an Errata Alert is applicable to one or more systems in his or her RHN account, as well as daily summaries of system events.
- RHN List Page Size — Maximum number of items that appear in a list on a single page. If more items are in the list, clicking the **Next** button displays the next group of items. This preference applies to the user's view of system lists, Errata lists, package lists, and so on.
- Time Zone — Set this user's time zone so that scheduled actions are arranged according to the time in the relevant time zone.
- Red Hat Contact Options — Identify what ways (email, phone, fax, or mail) Red Hat may contact the user.

To modify any of these options, make your changes and click the **Save Preferences** button.

6.8.1.1.6. User List ⇒ Active ⇒ User Details ⇒ Addresses —

This tab lists the addresses associated with the user's account. To update this information, click the appropriate **Edit this address** link, enter the relevant information, and click the **Update** button.

6.8.1.1.7. User List ⇒ Active ⇒ User Details ⇒ Notification Methods —

This tab lists email and pager addresses designated to receive alerts from Monitoring probes. To create a method, click **create new method** and complete the fields. If you will receive these alerts via pager, select the associated checkbox to have the messages sent in a shorter format. When finished, click **Create Method**. The method shows up in the Methods list, from which it can be edited and deleted.

You may delete notification methods here, as well. If the notification method has probes attached to it, you are presented with a list of the probes. Note that if you are a Monitoring Administrator and cannot manage the system in question, the **System Details** and probe's **Current State** page are not accessible via links in their names. As always, Organization Administrators have full access to all aspects of your RHN account.

6.8.2. User List ⇒ Deactivated —

This page lists all users who have been deactivated. To reactivate any of the users listed here, click the check box to the left of their name and click the **Reactivate** button followed by the **Confirm** button. Reactivated users retain the permissions and system group associations they had when they were deactivated. Clicking on the User Name of any individual takes you to their User Details page.

6.8.3. User List ⇒ All —

The **All** page lists all users that belong to your organization. In addition to the fields listed in the previous two screens, the table of users includes a **Status** field. This field indicates whether the user is **Active** or **Deactivated**. Deactivated users are also grayed out to indicate their status. Click on the username to move to the user's **User Details** page.

6.9. Monitoring —

If you click the **Monitoring** tab on the top navigation bar, the **Monitoring** category and links appear. These pages, which require Monitoring entitlements, enable you to view the results of probes you have

set to run against Monitoring-entitled systems and manage the configuration of your monitoring infrastructure.

Initiate monitoring of a system through the **Probes** tab of the **System Details** page. Refer to Section 6.4.2.9, "System Details" for a description of the tab. See Appendix C, *Probes* for the complete list of available probes.

6.9.1. Probe Status —

The **Probe Status** page is shown by default when you click **Monitoring** in the top navigation bar.

The **Probe Status** page displays the summary count of probes in the various states and provides a simple interface to find problematic probes quickly. Please note that the probe totals in the tabs at the top of the page may not match the numbers of probes displayed in the tables below. The counts at the top include probes for all systems in your organization, while the tables display probes on only those systems to which you have access through the System Group Administrator role. Also, the probe counts displayed here may be out of sync by as much as one minute.

The following list describes each state and identifies the icons associated with them:

- — *Critical* - The probe has crossed a CRITICAL threshold.
- — *Warning* - The probe has crossed a WARNING threshold.
- — *Unknown* - The probe is not able to accurately report metric or state data.
- — *Pending* - The probe has been scheduled but has not yet run or is unable to run.
- — *OK* - The probe is running successfully.

The **Probe Status** page contains tabs for each of the possible states, as well as one that lists all probes. Each table contains columns indicating probe state, the monitored system, the probes used, and the date and time the status was last updated.

In these tables, clicking the name of the system takes you to the **Probes** tab of the **System Details** page. Clicking the name of the probe takes you to its **Current State** page. From there, you may edit the probe, delete it, and generate reports based upon its results.

Monitoring data and probe status information that was previously availble only through the web interface of the Satellite can now be exported as a CSV file. Click on the **Download CSV** links throughout the Monitoring pages to download CSV files of relevent information. The exported data may include, but is not limited to:

- Probe status
- All probes in a given state (OK, WARN, UNKNOWN, CRITICAL, PENDING)
- A Probe Event history

6.9.1.1. Probe Status ⇒ Critical —

The probes that have crossed their CRITICAL thresholds or reached a critical status by some other means. For instance, some probes become critical (rather than unknown) when exceeding their timeout period.

6.9.1.2. Probe Status ⇒ Warning —

The probes that have crossed their WARNING thresholds.

6.9.1.3. Probe Status ⇒ Unknown —

The probes that cannot collect the metrics needed to determine probe state. Most but not all probes enter an unknown state when exceeding their timeout period. This may mean that the timeout period should be increased, or the connection cannot be established to the monitored system.

It is also possible the probes' configuration parameters are not correct and their data cannot be found. Finally, this state may indicate that a software error has occurred.

6.9.1.4. Probe Status ⇒ Pending —

The probes whose data have not been received by RHN. This state is expected for a probe that has just been scheduled but has not yet run. If all probes go into a pending state, your monitoring infrastructure may be failing.

6.9.1.5. Probe Status ⇒ OK —

The probes that have run successfully without exception. This is the state desired for all probes.

6.9.1.6. Probe Status ⇒ All —

All probes scheduled on systems in your account, listed in alphabetical order by the name of system.

6.9.1.7. Current State —

Identifies the selected probe's status and when it last ran, while providing the ability to generate a report on the probe. Although this page is integral to monitoring, it is found under the **Probes** tab within the **System Details** page since its configuration is specific to the system being monitored.

To view a report of the probe's results, choose a relevant duration using the **date** fields and decide whether you would like to see metric data, the state change history or both. To obtain metric data, select the metric(s) on which you wish to see a report, and decide (using the checkboxes) whether the results should be shown in a graph, an event log, or both. Then click **Generate report** at the bottom of the page. If no data exist for the probe's metrics, you are presented with the following message: **NO DATA SELECTED TIME PERIOD AND METRIC**.

6.9.2. Notification —

Identifies the contact methods that have been established for your organization. These methods contain email or pager addresses designated to receive alerts from probes.

The various notification methods available to your organization are listed here on the default **Notification** screen. The methods are listed according to the user to which they apply.

To create a new notification method, click on the name of the user to whom the notification will apply. The user's User Details ⇒ Notification Methods page appears. Refer to Section 6.8.1.1.7, “User List ⇒ Active ⇒ User Details ⇒ Notification Methods — ” for further information. Click on the title of the notification method to edit the properties of the method.

6.9.2.1. Notification ⇒ Filters

Notification filters allow you to create long-term rules that suspend, redirect, or automatically acknowledge standard notifications or send supplemental notifications. This can be helpful in managing

verbose or frequent probe communication.

6.9.2.1.1. Notification ⇒ Notification Filters ⇒ Active Filters

This is the default screen for the Notification Filters tab. It lists all active filters available for your organization. Click the name of the filter to edit the properties of the filter.

To create a notification filter, click the **create new notification filter** link in the upper right of the screen. Configure each option listed below and click the **Save Filter** button to create the filter.

1. *Description*: Enter a value that allows you to distinguish this filter from others.
2. *Type*: Determine what action the filter should take: redirect, acknowledge, suspend, or supplement the incoming notification.
3. *Send to*: The **Redirect Notification** and **Supplemental Notification** options in step two require an email address to which to send the notifications. The remaining options require no email address.
4. *Scope*: Determine which monitoring components are subject to the filter.
5. *Organization/Scout/Probe*: This option allows you to select the organization, scout(s), or probe(s) to which this filter applies. To select multiple items from the list, hold the **Ctrl** key while clicking the names of the items. To select a range of items, hold the **Shift** key while clicking on the first and last items in the range.
6. *Probes in State*: Select which probe state(s) relate to the filter. For example, you may choose to create a supplemental notification for critical probes only. Un-check the box to the left of any state you want the filter to ignore.
7. *Notifications sent to*: This is the method to which the notification would be sent if no filter were in place. You may, for example, redirect notifications that would normally go to a user should that individual go on vacation, leaving all other notifications from the probe unchanged.
8. *Match Output*: Select precise notification results by entering a regular expression here. If the "Message:" portion of the notification does not match the regular expression, the filter is not applied.
9. *Recurring*: Select whether a filter runs continuously or on a recurring basis. A recurring filter runs multiple times for a period of time smaller than the duration of the filter. For example, a recurring filter could run for 10 minutes of every hour between the start and end times of the filter. A non-recurring filter runs continuously between the start and end times of the filter.
10. *Beginning*: Enter a date and time for the filter to begin operation.
11. *Ending*: Enter an end date and time for the filter.
12. *Recurring Duration*: How long a recurring filter instance is active. This field, applicable to recurring filters only, begins at the **Beginning** time specified above. Any notification generated outside of the specified duration is not filtered.
13. *Recurring Frequency*: How often the filter activates.

Notification filters cannot be deleted. However, a filter may be canceled by setting the end date to some time in the past. (Note that the end date must be equal to or later than the start date, or the change fails.) Another method is to select a set of filters from the **Active** page and click the **Expire Notification Filters** button in the lower right. These filters are then canceled and appears in the **Expired Filters** tab.

6.9.2.1.2. Notification ⇒ Notification Filters ⇒ Expired Filters

This tab lists all notification filters whose end date has passed. Expired filters are stored indefinitely; this allows an organization to recycle useful filters as needed and provides a historical record for

troubleshooting.

6.9.3. Probe Suites

Probe Suites allow you to configure and apply one or more probes to a system or systems. Probe Suites may be configured once and then applied to any number of systems in a batch. This results in time savings and consistency for Monitoring customers.

To create and apply a Probe Suite, first create an empty Probe Suite, then configure member probes, and finally apply the Suite to selected systems.

1. From the Monitoring ⇒ Probe Suites page, select the **`create probe suite`** link. Enter an easily distinguishable name for the Probe Suite. You may also choose to add a brief description of the Suite. Click the **`Create Probe Suite`** button to continue.
2. Add and configure the probes that comprise the Suite. Click the **`create new probe`** link in the upper right.
3. As described in Section 6.4.2.9.5.2, “System Details ⇒ Monitoring — ”, configure the probe and click the **`Create Probe`** button in the lower right. Repeat this process until all desired probes have been added.

   Note

   Sendmail must be configured correctly on your RHN Satellite and each client system to which the Probe Suite is applied must have the **`rhnmd`** daemon installed and running. Refer to the *RHN Satellite Server 5.0.0 Installation Guide* for additional information.

4. Add the systems to which the Probe Suite applies. Click the **`add systems to probe suite`** link in the upper right of the screen to continue.
5. The next page displays a list of all systems with Monitoring entitlements. Check the box to the left of the system(s) to which you wish to apply the Probe Suite, select the monitoring scout you wish to use, and click the **`Add systems to probe suite`** button to complete the creation of the Probe Suite.

You can either delete or detach probes from the suite. Detaching a probe disassociates the probes from the suite and converts them to system-specific probes for the specified system. This means that changes to the detached probes only effect that system. Deleting a probe removes it from the Suite for all systems.

To remove probes from the Probe Suite:

1. From the Monitoring ⇒ Probe Suites page, click on the title of the Probe Suite you wish to alter.
2. Select the **`Probes`** sub-tab.
3. Check the box next to the probe you wish to remove.
4. Click the **`Delete probes from Probe Suites`** button.

You may also remove a system from the Probe Suite. There are two ways to accomplish this. The first method is to detach the system from the Probe Suite. When you do so, the system still has the same probes assigned to it. However, you now have the ability to configure these probes individually without affecting any other systems. For more information about removing probes from an individual system, refer to Section 6.4.2.9.5.2, “System Details ⇒ Monitoring — ”.

To detach a system from the suite:

1. From the **Monitoring** ⇒ **Probe Suites** page, click on the title of the Probe Suite you wish to alter.
2. Select the **Systems** sub-tab.
3. Check the box next to the system(s) you wish to remove from the Probe Suite.
4. Click the **Detach System(s) from Probe Suite** button

The second method is to remove the system from the suite. This removes the system from the suite and deletes all running probes from the system.

Note

This action deletes all of the Probe Suites' probes from the system as well as all of the historical Time Series and Event Log data. This action is irreversible.

To remove a system from the Probe Suite and delete all associated probes from the system:

1. From the Monitoring ⇒ Probe Suites page, click on the title of the Probe Suite you wish to alter.
2. Select the **Systems** sub-tab.
3. Check the box next to the system(s) you wish to remove from the Probe Suite.
4. Click the **Remove System(s) from Probe Suite** button.

Finally, as with single Probes, you may download a CSV file containing information about Probe Suites. Click the **Download CSV** link at the bottom of the **Monitoring** ⇒ **Probe Suites** page to download the file.

6.9.4. Scout Config Push —

Displays the status of your monitoring infrastructure. Anytime you make a change to your monitoring configuration, such as adding a probe to a system or editing a probe's thresholds, you must reconfigure your monitoring infrastructure. Do this by selecting the RHN Server's checkbox and clicking **Push Scout Configs**. The table on this page identifies the date and time of requested and completed pushes.

Clicking the name of the server opens its Red Hat Network Monitoring Daemon SSH Public Key. This allows you to copy and paste the SSH key to the systems that are monitored by the scout. This is required in order for the Red Hat Network Monitoring Daemon to connect to the Satellite.

6.9.5. General Config —

Collects information that is universally applicable to your Monitoring infrastructure.Modifying anything on this page causes the Monitoring services on the RHN Satellite to reset. It also schedules restart events for the Monitoring services on all Monitoring-enabled RHN Proxy Servers that connect to this Satellite. This is done so that the Monitoring services on these servers immediately reload their configuration.

Typically, the defaults provided in other fields are acceptable, since they are derived from your Satellite installation. Nevertheless, you may use the fields on this page to alter your Monitoring configuration. For instance, you may change your mail exchange server here. This page also allows you to alter the destination of all administrative emails from the Satellite. When finished, click **Update Config**.

6.10. Satellite Tools

This page allows RHN Satellite customers to manage the basic configuration of their Satellite. The default page, **Task Engine Status**, provides a summary of the latest execution times for key tasks.

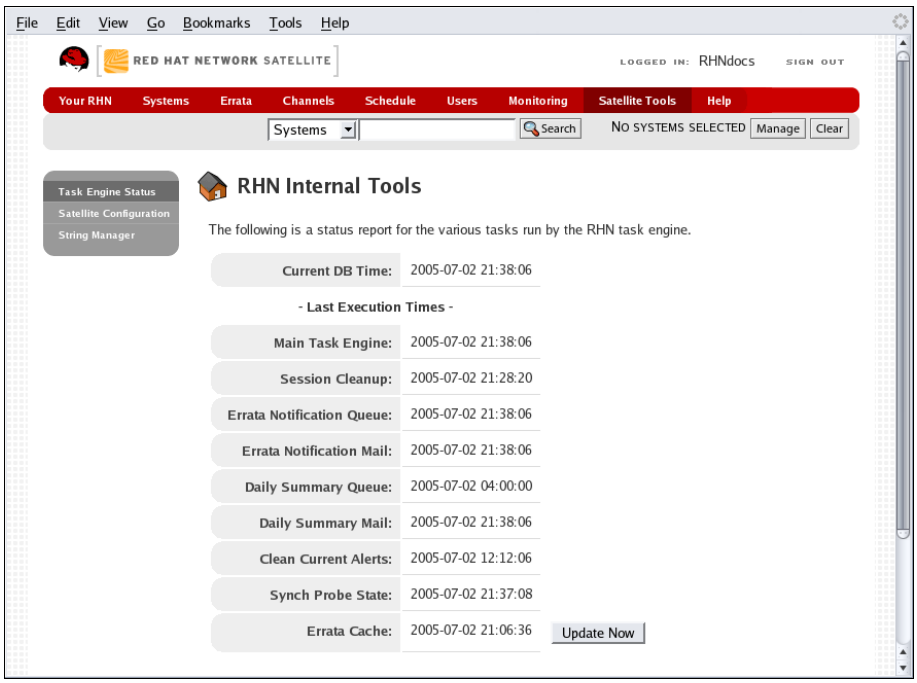

File Edit View Go Bookmarks Tools Help
RED HAT NETWORK SATELLITE
LOGGED IN: RHNdocs SIGN OUT
Your RHN Systems Errata Channels Schedule Users Monitoring Satellite Tools Help
Systems Search NO SYSTEMS SELECTED Manage Clear
Task Engine Status
Satellite Configuration
String Manager
RHN Internal Tools
The following is a status report for the various tasks run by the RHN task engine.
Current DB Time: 2005-07-02 21:38:06
- Last Execution Times -
Main Task Engine: 2005-07-02 21:38:06
Session Cleanup: 2005-07-02 21:28:20
Errata Notification Queue: 2005-07-02 21:38:06
Errata Notification Mail: 2005-07-02 21:38:06
Daily Summary Queue: 2005-07-02 04:00:00
Daily Summary Mail: 2005-07-02 21:38:06
Clean Current Alerts: 2005-07-02 12:12:06
Synch Probe State: 2005-07-02 21:37:08
Errata Cache: 2005-07-02 21:06:36
Update Now

Figure 6.19. Satellite Tools

6.10.1. Satellite Tools ⇒ Satellite Configuration

This tab is broken down into subtabs that allow you to configure most aspects of the RHN Satellite. Once changes have been made, it is important to restart the Satellite, which may be accomplished on the final tab.

6.10.1.1. Satellite Tools ⇒ Satellite Configuration ⇒ General

The **Satellite Configuration ⇒ General Configuration** page allows you to alter the most basic Satellite settings, such as the admin email address and whether Monitoring is enabled.

6.10.1.2. Satellite Tools ⇒ Satellite Configuration ⇒ Monitoring

The **RHN Satellite Configuration ⇒ Monitoring** page allows you to configure the monitoring aspects of this Satellite. The local mail exchanger and local main domain are used to mail monitoring notification messages to administration. This is required only if you intend to receive alert notifications from probes. If you do, provide the mail server (exchanger) and domain to be used. Note that **sendmail** must be configured to handle email redirects of notifications. When finished, click **Update Config**.

6.10.1.3. Satellite Tools ⇒ Satellite Configuration ⇒ Certificate

The **RHN Satellite Configuration ⇒ Certificate** page allows you to either upload a new Satellite certificate. To identify the certificate's path, click **Browse**, navigate to the file, and select it. To input its contents, open your certificate in a text editor, copy all lines, and paste them directly into the large text field at the bottom. Red Hat recommends using the file locator as it is less error prone. Click **Validate Certificate** to continue. If you receive errors related to DNS, ensure your Satellite is configured correctly.

6.10.1.4. Satellite Tools ⇒ Satellite Configuration ⇒ Bootstrap

The **RHN Satellite Configuration ⇒ Bootstrap** page allows you to generate a bootstrap script for redirecting client systems from the central RHN Servers to the Satellite. This script, to be placed in the **/var/www/html/pub/bootstrap/** directory of the Satellite, significantly reduces the effort involved in reconfiguring all systems, which by default obtain packages from the central RHN Servers. The required fields are pre-populated with values derived from previous installation steps. Ensure this information is accurate.

Checkboxes offer options for including built-in security SSL and GNU Privacy Guard (GPG) features, both of which are advised. In addition, you may enable remote command acceptance and remote configuration management of the systems to be bootstrapped here. Both features are useful for completing client configuration. Finally, if you are using an HTTP proxy server, complete the related fields. When finished, click **Generate Bootstrap Script**.

6.10.1.5. Satellite Tools ⇒ Satellite Configuration ⇒ Restart

The **RHN Satellite Configuration ⇒ Restart** page contains the final step in configuring the Satellite. Click the **Restart** button to restart the Satellite in order to incorporate all of the configuration options added on the previous screens. Note that it will take between four and five minutes for the restart to finish.

6.11. Help

The **Help** pages provide access to the full suite of documentation and support available to RHN users. Click **Help** in the **Your RHN** category to see a list of options available to you.

6.11.1. Help Desk

The **Help Desk** page summarizes the help options available within this section. Click either the links within this page or the buttons on the left navigation bar to explore further.

6.11.2. Quick Start Guide

The **Quick Start Guide** page contains a brief overview of Red Hat Network and its many features. If you are unfamiliar with RHN, it is recommended you read this guide in its entirety. Topics covered include registering your systems, applying Errata Updates, using one-click updates, and troubleshooting.

6.11.3. FAQ

The **FAQ** page lists Frequently Asked Questions and answers to those questions. These are broken down into the following categories, each represented by a separate button and page: Top Ten, General, Account Management, Getting Started, Service Levels, Using RHN, Technical Questions, Management Service, Privacy/Legal, Policies, Definitions, and All.

6.11.4. Migration FAQ

Frequently Asked Questions regarding migration from RHL end-of-life products.

6.11.5. Reference Guide

The **Reference Guide** page takes you to this same document, the most comprehensive set of instructions for using Red Hat Network. Note that links to other technical guides may also appear in the left navigation bar, depending on the entitlement level and product offering of the account with which you logged in.

6.11.6. Best Practices Guide

A set of best practices for corporate RHN users.

6.11.7. Contact RHN

The **Contact RHN** page provides methods by which customers may obtain help. Specifically, logged out users have access to the FAQ, Customer Service email address, and rhn-users mailing list. Logged in paid users have access to all of the above and an online form that can be submitted to rhn-feedback or the Customer Service address. In addition, the online form enables them to submit requests for technical support.

The Customer Service address handles billing and purchasing questions, while the rhn-users list enables customers to help one another. The rhn-feedback address collects customer input and provides an auto response, but nothing more. The technical support form ensures the customer will get a personalized and helpful response in a timely manner.

6.11.8. Satellite Installation Guide

Detailed information regarding RHN Satellite server and its installation.

6.11.9. Proxy Guide

Detailed information regarding RHN Proxy server.

6.11.10. Client Configuration Guide

Documentation for setting up clients to connect to an RHN Proxy or Satellite server.

6.11.11. Channel Management Guide

Documentation for the creation and maintenance of custom channels using RHN.

6.11.12. Terms &Conditions

The **Terms &Conditions** page displays the RHN Network Services Use and Subscription Agreement.

6.11.13. Outage Policy

The **Outage Policy** page identifies scheduled maintenance windows for Red Hat Network and provides the means to subscribe to the Email Outage List (rhn-outage-list@redhat.com) to be notified of emergency and other unscheduled outages.

6.11.14. Release Notes

The **Release Notes** page lists the notes accompanying every recent release of Red Hat Network. These notes describe all significant changes occurring in a given release cycle, from major enhancements to the user interface to minor changes to the related documentation.

6.11.15. Get RHN Software

The **RHN Software** page provides direct links to the **Red Hat Update Agent** and **Red Hat Network Registration Client** for every supported distribution. In addition, it describes how to resolve expired Secure Sockets Layers (SSL) certificates if you are using an older version of Red Hat Enterprise Linux that shipped with a certificate that is now expired.

Chapter 7. Monitoring

The Red Hat Network Monitoring entitlement allows you to perform a whole host of actions designed to keep your systems running properly and efficiently. With it, you can keep close watch on system resources, network services, databases, and both standard and custom applications.

Monitoring provides both real-time and historical state-change information, as well as specific metric data. You are not only notified of failures immediately and warned of performance degradation before it becomes critical, but you are also given the information necessary to conduct capacity planning and event correlation. For instance, the results of a probe recording CPU usage across systems would prove invaluable in balancing loads on those systems.

Monitoring entails establishing notification methods, installing probes on systems, regularly reviewing the status of all probes, and generating reports displaying historical data for a system or service. This chapter seeks to identify common tasks associated with the Monitoring entitlement. Remember, virtually all changes affecting your Monitoring infrastructure must be finalized by updating your configuration, through the **Scout Config Push** page.

7.1. Prerequisites

Before attempting to implement RHN Monitoring within your infrastructure, ensure you have all of the necessary tools in place. At a minimum, you need:

- Monitoring entitlements — These entitlements are required for all systems that are to be monitored. Monitoring is supported only on Red Hat Enterprise Linux systems.
- RHN Satellite with Monitoring — Monitoring systems must be connected to a Satellite with a base operating system of Red Hat Enterprise Linux AS 3 Update 5, Red Hat Enterprise Linux AS 4, or later. Refer to the RHN Satellite Installation Guide within **Help** for installation instructions. Contact a Red Hat sales representative to purchase Satellite.
- Monitoring Administrator — This role must be granted to users installing probes, creating notification methods, or altering the monitoring infrastructure in any way. (Remember, the Organization Administrator automatically inherits the abilities of all other roles within an organization and can therefore conduct these tasks.). Assign this role through the **User Details** page for the user.
- Red Hat Network Monitoring Daemon — This daemon, along with the SSH key for the scout, is required on systems that are monitored in order for the internal process monitors to be executed. You may, however, be able to run these probes using the systems' existing SSH daemon (**sshd**). Refer to Section 7.2, “Red Hat Network Monitoring Daemon (**rhnmd**)” for installation instructions and a quick list of probes requiring this secure connection. Refer to Appendix C, *Probes* for the complete list of available probes.

7.2. Red Hat Network Monitoring Daemon (rhnmd)

To get the most out of your Monitoring entitlement, Red Hat suggests installing the Red Hat Network Monitoring Daemon on your client systems. Based upon **OpenSSH**, **rhnmd** enables the RHN Satellite to communicate securely with the client system to access internal processes and retrieve probe status.

Please note that the Red Hat Network Monitoring Daemon requires that monitored systems allow connections on port 4545. You may avoid opening this port and installing the daemon altogether by using **sshd** instead. Refer to Section 7.2.3, “Configuring SSH” for details.

7.2.1. Probes requiring the daemon

An encrypted connection, either through the Red Hat Network Monitoring Daemon or **sshd**, is required on client systems for the following probes to run:

- Linux::CPU Usage
- Linux::Disk IO Throughput
- Linux::Disk Usage
- Linux::Inodes
- Linux::Interface Traffic
- Linux::Load
- Linux::Memory Usage
- Linux::Process Counts by State
- Linux::Process Count Total
- Linux::Process Health
- Linux::Process Running
- Linux::Swap Usage
- Linux::TCP Connections by State
- Linux::Users
- Linux::Virtual Memory
- LogAgent::Log Pattern Match
- LogAgent::Log Size
- Network Services::Remote Ping
- Oracle::Client Connectivity
- General::Remote Program
- General::Remote Program with Data

Note that all probes in the Linux group have this requirement.

7.2.2. Installing the Red Hat Network Monitoring Daemon

Install the Red Hat Network Monitoring Daemon to prepare systems for monitoring with the probes identified in Section 7.2.1, “Probes requiring the daemon”. Note that the steps in this section are optional if you intend to use **sshd** to allow secure connections between the RHN monitoring infrastructure and the monitored systems. Refer to Section 7.2.3, “Configuring SSH” for instructions.

The **rhnmd** package can be found in the RHN Tools channel for all Red Hat Enterprise Linux distributions. To install it:

1. Subscribe the systems to be monitored to the RHN Tools channel associated with the system. This can be done individually through the **System Details** ⇒ **Channels** ⇒ **Software** subtab or for multiple systems at once through the **Channel Details** ⇒ **Target Systems** tab.
2. Once subscribed, open the **Channel Details** ⇒ **Packages** tab and find the **rhnmd** package (under 'R').
3. Click the package name to open the **Package Details** page. Go to the **Target Systems** tab, select the desired systems, and click **Install Packages**.
4. Install the SSH public key on all client systems to be monitored, as described in Section 7.2.4, “Installing the SSH key”.
5. Start the Red Hat Network Monitoring Daemon on all client systems using the command:

```
service rhnmd start
```

6. When adding probes requiring the daemon, accept the default values for **RHNMD User** and **RHNMD Port**: **nocpulse** and **4545**, respectively.

7.2.3. Configuring SSH

If you wish to avoid installing the Red Hat Network Monitoring Daemon and opening port 4545 on client systems, you may configure **sshd** to provide the encrypted connection required between the systems and RHN. This may be especially desirable if you already have **sshd** running. To configure the daemon for monitoring use:

1. Ensure the SSH package is installed on the systems to be monitored:

```
rpm -qi openssh-server
```

2. Identify the user to be associated with the daemon. This can be any user available on the system, as long as the required SSH key can be put in the user's **~/.ssh/authorized_keys** file.
3. Identify the port used by the daemon, as identified in its **/etc/ssh/sshd_config** configuration file. The default is port 22.
4. Install the SSH public key on all client systems to be monitored, as described in Section 7.2.4, “Installing the SSH key”.
5. Start the **sshd** on all client systems using the command:

```
service sshd start
```

6. When adding probes requiring the daemon, insert the values derived from steps 2 and 3 in the **RHNMD User** and **RHNMD Port** fields.

7.2.4. Installing the SSH key

Whether you use **rhnmd** or **sshd**, you must install the Red Hat Network Monitoring Daemon public SSH key on the systems to be monitored to complete the secure connection. To install it:

1. Navigate to the **Monitoring ⇒ Scout Config Push** page of the RHN website and click the name of the RHN Server that will monitor the client system. The SSH **id_dsa.pub** key is visible on the resulting page.
2. Copy the character string (beginning with **ssh-dss** and ending with the hostname of the RHN Server).
3. On the command line of the system to be monitored, switch to the user aligned with the daemon. This is accomplished for **rhnmd** with the command:

```
su - nocpulse
```

4. Paste the key character string into the **~/.ssh/authorized_keys** file for the daemon's user. For **rhnmd**, this is **/opt/nocpulse/.ssh/authorized_keys**.

   If config management is enabled on the systems to be monitored, you may deploy this file across systems using a config channel. Refer to Section 6.6.6.1, “Preparing Systems for Config Management” for details.

Note

If valid entries already exist in **authorized_keys**, add the daemon key to the file rather than replacing the existing key. To do so, save the copied text to **id_dsa.pub** in the same **.ssh/** directory and then run the following command: **cat ~/.ssh/id_dsa.pub >> ~/.ssh/authorized_keys**.

5. Finally, ensure the **.ssh/** directory and **authorized_keys** file have the appropriate permissions set. This can be done as the daemon's user with the following commands:

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
```

Once the key is in place and accessible, all probes that require it should allow **ssh** connections between the Monitoring infrastructure and the monitored system. You may then schedule probes requiring the monitoring daemon to run against the newly configured systems.

7.3. mysql-server package

If your RHN Satellite will serve Monitoring-entitled client systems against which you wish to run **MySQL** probes, you must configure the **mysql-server** package on the RHN Satellite. Refer to Appendix C, *Probes* for a listing of all available probes.

Subscribe the Satellite to the Red Hat Enterprise Linux AS Extras channel and install the **mysql-server** package either through the RHN website or via **up2date**.

Two additional packages will also be downloaded in the transaction. These are needed for the **mysql-server** package to be installed and run successfully. Once finished, your Satellite may be used to schedule **MySQL** probes.

7.4. Notifications

In addition to viewing probe status within the RHN interface, you may be notified whenever a probe changes state. This is especially important when monitoring mission-critical production systems. For this reason, Red Hat recommends taking advantage of this feature.

To enable probe notifications within RHN, you must have identified a mail exchange server and mail domain during installation of your RHN Satellite and configured **sendmail** to properly handle incoming mail. Refer to the *Installation* chapter of the *RHN Satellite Installation Guide* for details.

7.4.1. Creating Notification Methods

Notifications are sent via a *notification method*, an email or pager address associated with a specific RHN user. Although the address is tied to a particular user account, it may serve multiple administrators through an alias or mailing list. Each user account can contain multiple notification methods. To create a notification method:

1. Log into the RHN website as either an Organization Administrator or Monitoring Administrator.
2. Navigate to the **User Details ⇒ Notification Methods** tab and click **create new method**.

3. Enter an intuitive, descriptive label for the method name, such as **DBA day email**, and provide the correct email or pager address. Remember, the labels for all notification methods are available in a single list during probe creation, so they should be unique to your organization.
4. Select the checkbox if you desire abbreviated messages to be sent to the pager. This shorter format contains only the probe state, system hostname, probe name, time of message, and Send ID. The standard, longer format displays additional message headers, system and probe details, and instructions for response.
5. When finished, click **Create Method**. The new method shows up in the **User Details ⇒ Notification Methods** tab and the **Notification** page under the top **Monitoring** category. Click its name to edit or delete it.
6. While adding probes, select the **Probe Notifications** checkbox and select the new notification method from the resulting pulldown menu. Notification methods assigned to probes cannot be deleted until they are dis-associated from the probe.

7.4.2. Receiving Notifications

If you create notification methods and associate them with probes, you must be prepared to receive them. These notifications come in the form of brief text messages sent to either email or pager addresses. Here is an example of an email notification:

```
 Subject: CRITICAL: [hostname]: Satellite: Users at 1 From: "Monitoring
Satellite Notification" (rogerthat01@redhat.com) Date: Mon, 6 Dec 2004
13:42:28 -0800 To: user@organization.com This is RHN Monitoring Satellite
notification 01dc8hqw. Time: Mon Dec 06, 21:42:25 PST State: CRITICAL System:
[hostname] ([IP address]) Probe: Satellite: Users Message: Users 6 (above
critical threshold of 2) Notification #116 for Users Run from: RHN Monitoring
Satellite
```

As you can see, the longer email notifications contain virtually everything you would need to know about the associated probe. In addition to the probe command, run time, system monitored, and state, the message contains the *Send ID*, which is a unique character string representing the precise message and probe. In the above message, the Send ID is **01dc8hqw**.

Pager notifications, by necessity, contain only the most important details, namely the subject of the email message (containing state, system, probe, and time) and the Send ID. Here is an example pager notification:

```
CRITICAL: [hostname]: Satellite: Users at 21:42 PST, notification 01dc8hqw
```

7.4.3. Redirecting Notifications

Upon receiving a notification, you may redirect it by including advanced notification rules within an acknowledgment email. Just reply to the notification and include the desired option. These are the possible redirect options, or *filter types*:

- ACK METOO — Sends the notification to the redirect destination(s) *in addition to* the default destination.
- ACK SUSPEND — Suspends the notification method for a specified time period.
- ACK AUTOACK — Does not change the destination of the notification, but automatically acknowledges matching alerts as soon as they are sent.
- ACK REDIR — Sends the notification to the redirect destination(s) *instead of* the default destination.

The format of the rule should be ***filter_type probe_type duration email_address*** where ***filter_type*** indicates one of the previous advanced commands, ***probe_type*** indicates probe or system, ***duration*** indicates the length of time for the redirect, and ***email_address*** indicates the intended recipient. For example:

```
ACK METOO system 1h boss@domain.com
```

Capitalization is not required. Duration can be listed in minutes (m), hours (h), or days (d). Email addresses are needed only for redirects (REDIR) and supplemental (METOO) notifications.

The description of the action contained in the resulting email defaults to the command entered by the user. The reason listed is a summary of the action, such as **email ack redirect by user@domain.com** where user equals the sender of the email.

Note

You can halt or redirect almost all probe notifications by replying to a notification emails with a variation of the command **ack suspend host**. However, you cannot halt Satellite probe notifications by responding to a probe with **ack suspend host** or other redirect responses. These probes require you to change the notifications within the web interface of the Satellite.

7.4.4. Filtering Notifications

Since notifications can be generated whenever a probe changes state, simple changes in your network can result in a flood of notifications. The creation, cancellation, and application of Notification filters is discussed in detail in Section 6.9.2.1, “Notification ⇒ Filters”.

7.4.5. Deleting Notification Methods

Theoretically, removing notification methods should be as easy as creating them. After all, you must populate no fields to conduct the deletion and a button exists for this explicit purpose. However, existing relationships between methods and probes can complicate this process. Follow these steps to remove a notification method:

1. Log into the RHN website as an Organization Administrator or Monitoring Administrator.
2. Navigate to the **Monitoring ⇒ Notifications** page and click the name of the method to be removed.
3. On the **User Details ⇒ Notification Methods** tab, click **delete method**. If the method is not associated with any probes, you are presented with a confirmation page. Click **Confirm Deletion**. The notification method is removed.

   Tip

   Since both the notification method name and address can be edited, consider updating the method rather than deleting it. This redirects notifications from all probes using the method without having to edit each probe and create a new notification method.

4. If the method is associated with one or more probes, you are presented with a list of the probes using the method and the systems to which the probes are attached instead of a confirmation page. Click the probe name to go directly to the **System Details ⇒ Probes** tab.

5. On the **System Details ⇒ Probes** tab, select another notification method and click **Update Probe**.
6. You may now return to the **Monitoring ⇒ Notifications** page and delete the notification method.

7.5. Probes

Now that the Red Hat Network Monitoring Daemon has been installed and notification methods have been created, you may begin installing probes on your Monitoring-entitled systems. If a system is entitled to Monitoring, a **Probes** tab appears within its **System Details** page. This is where you will conduct most probe-related work.

7.5.1. Managing Probes

To add a probe to a system, the system must be entitled to Monitoring. Further, you must have access to the system itself, either as the system's root user, through the System Group Administrator role, or as the Organization Administrator. Then:

1. Log into the RHN website as either an Organization Administrator or the System Group Administrator for the system.
2. Navigate to the **System Details ⇒ Probes** tab and click **create new probe**.
3. On the **System Probe Creation** page, complete all required fields. First, select the Probe Command Group. This alters the list of available probes and other fields and requirements. Refer to Appendix C, *Probes* for the complete list of probes by command group. Remember that some probes require the Red Hat Network Monitoring Daemon to be installed on the client system.
4. Select the desired Probe Command and the Monitoring Scout, typically **RHN Monitoring Satellite** but possibly an RHN Proxy Server. Enter a brief but unique description for the probe.
5. Select the **Probe Notifications** checkbox to receive notifications when the probe changes state. Use the **Probe Check Interval** pulldown menu to determine how often notifications should be sent. Selecting **1 minute** (and the **Probe Notification** checkbox) means you will receive notifications every minute the probe surpasses its CRITICAL or WARNING thresholds. Refer to Section 7.4, “Notifications” to find out how to create notification methods and acknowledge their messages.
6. Use the **RHNMD User** and **RHNMD Port** fields, if they appear, to force the probe to communicate via **sshd**, rather than the Red Hat Network Monitoring Daemon. Refer to Section 7.2.3, “Configuring SSH” for details. Otherwise, accept the default values of **nocpulse** and **4545**, respectively.
7. If the **Timeout** field appears, review the default value and adjust to meet your needs. Most but not all timeouts result in an UNKNOWN state. If the probe's metrics are time-based, ensure the timeout is not less than the time alloted to thresholds. Otherwise, the metrics serve no purpose, as the probe will time out before any thresholds are crossed.
8. Use the remaining fields to establish the probe's alert thresholds, if applicable. These CRITICAL and WARNING values determine at what point the probe has changed state. Refer to Section 7.5.2, “Establishing Thresholds” for best practices regarding these thresholds.
9. When finished, click **Create Probe**. Remember, you must commit your Monitoring configuration change on the **Scout Config Push** page for this to take effect.

To delete a probe, navigate to its **Current State** page (by clicking the name of the probe from the **System Details ⇒ Probes** tab), and click **delete probe**. Finally, confirm the deletion.

7.5.2. Establishing Thresholds

Many of the probes offered by RHN contain alert thresholds that, when crossed, indicate a change in state for the probe. For instance, the Linux::CPU Usage probe allows you to set CRITICAL and WARNING thresholds for the percent of CPU used. If the monitored system reports 75 percent of its CPU used, and the WARNING threshold is set to 70 percent, the probe will go into a WARNING state. Some probes offer a multitude of such thresholds.

In order to get the most out of your Monitoring entitlement and avoid false notifications, Red Hat recommends running your probes without notifications for a time to establish baseline performance for each of your systems. Although the default values provided for probes may suit you, every organization has a different environment that may require altering thresholds.

7.5.3. Monitoring the RHN Server

In addition to monitoring all of your client systems, you may also use RHN to monitor your RHN Server, whether that be an RHN Satellite a RHN Proxy Server. To monitor your RHN Server, find a system monitored by the server, and go to that system's **System Details ⇒ Probes** tab.

Click **create new probe** and select the **Satellite** Probe Command Group. Next, complete the remaining fields as you would for any other probe. Refer to Section 7.5.1, “Managing Probes” for instructions.

Although the RHN Server appears to be monitored by the client system, the probe is actually run from the server on itself. Thresholds and notifications work normally.

Note

Any probes that require Red Hat Network Monitoring Daemon connections cannot be used against a RHN Satellite or RHN Proxy Server on which Monitoring software is running. This includes most probes in the Linux command group as well as the Log Agent probes and the Remote Program probes. Use the Satellite command group probes to monitor RHN Satellites and RHN Proxy Servers. In the case of Proxy scouts, the probes are listed under the system for which they are reporting data.

7.6. Troubleshooting

Though all Monitoring-related activities are conducted through the RHN website, Red Hat provides access to some command line diagnostic tools that may help you determine the cause of errors. To use these tools, you must be able to become the **nocpulse** user on the RHN Server conducting the monitoring.

First log into the RHN Server as root. Then switch to the **nocpulse** user with the following command:

```
su - nocpulse
```

You may now use the diagnostic tools described within the rest of this section.

7.6.1. Examining Probes with `rhn-catalog`

To thoroughly troubleshoot a probe, you must first obtain its probe ID. You may obtain this information by running **rhn-catalog** on the RHN Server as the **nocpulse** user. The output will resemble:

```
 2 ServiceProbe on example1.redhat.com (199.168.36.245): test 2 3 ServiceProbe
on example2.redhat.com (199.168.36.173): rhel2.1 test 4 ServiceProbe on
example3.redhat.com (199.168.36.174): SSH 5 ServiceProbe on
example4.redhat.com (199.168.36.175): HTTP
```

The probe ID is the first number, while the probe name (as entered in the RHN website) is the final entry on the line. In the above example, the **5** probe ID corresponds to the probe named **HTTP**.

Further, you may pass the **--commandline** (**-c**) and **--dump** (**-d**) options along with a probe ID to **rhn-catalog** to obtain additional details about the probe, like so:

```
rhn-catalog --commandline --dump 5
```

The **--commandline** option yields the command parameters set for the probe, while **--dump** retrieves everything else, including alert thresholds and notification intervals and methods.

The command above will result in output similar to:

```
 5 ServiceProbe on example4.redhat.com (199.168.36.175 ): linux:cpu usage Run
as: Unix::CPU.pm --critical=90 --sshhost=199.168.36.175 --warn=70 --timeout=15
--sshuser=nocpulse --shell=SSHRemoteCommandShell --sshport=4545
```

Now that you have the ID, you use it with **rhn-rhnprobe** to examine the probe's output. Refer to Section 7.6.2, “Viewing the output of **rhn-runprobe**” for instructions.

7.6.2. Viewing the output of rhn-runprobe

Now that you have obtained the probe ID with **rhn-catalog**, use it in conjunction with **rhn-runprobe** to examine the complete output of the probe. Note that by default, **rhn-runprobe** works in test mode, meaning no results are entered in the database. Here are its options:

Table 7.1. rhn-runprobe Options

Option	Description
--help	List the available options and exit.
--probe=*PROBE_ID*	Run the probe with this ID.
--prob_arg=*PARAMETER*	Override any probe parameters from the database.
--module=*PERL_MODULE*	Package name of alternate code to run.
--log=all=*LEVEL*	Set log level for a package or package prefix.
--debug=*LEVEL*	Set numeric debugging level.
--live	Execute the probe, enqueue data and send out notifications (if needed).

At a minimum, you should include the **--probe** option, the **--log** option, and values for each. The **--probe** option takes the probeID as its value and the **--log** option takes the value "all" (for all run levels) and a numeric verbosity level as its values. Here is an example:

```
rhn-runprobe --probe=5 --log=all=4
```

The above command requests the probe output for probeID 5, for all run levels, with a high level of

verbosity.

More specifically, you may provide the command parameters derived from **rhn-catalog**, like so:

```
rhn-runprobe 5 --log=all=4 --sshuser=nocpulse --sshport=4545
```

This yields verbose output depicting the probe's attempted execution. Errors are clearly identified.

Chapter 8. Virtualization

In order to manage and provision your client systems, you must first synchronize content from RHN's central servers to your Satellite.

RHN recommends that you sync at least the following channels:

- Red Hat Network Tools for RHEL Server (v. 5 for 32-bit x86) — rhn-tools-rhel-i386-server-5
- RHN Tools — rhn-tools-rhel-4-as-i386
- Red Hat Enterprise Linux Server (v. 5 for 32-bit x86) — rhel-i386-server-5 (and all child channels)
- Red Hat Enterprise Linux Server Virtualization (v. 5 for 32-bit x86) — rhel-i386-server-vt-5 (and all child channels)

8.1. Setting Up the Host System for Your Virtual Systems

Before creating guest systems, you must first prepare your host system. To do this, create a Red Hat Enterprise Linux 5 Server kickstart profile, then use that kickstart profile to install the operating system on your host. Once these steps are complete, you can proceed to provision virtual guests.

8.1.1. Create a Kickstart Profile for the Guest Systems

1. Login to the Satellite's web interface. Navigate to the **`Kickstart Overview`** screen by clicking the **`Manage Kickstarts`** link in the **`Tasks`** widget in **`Your RHN`**, or by clicking on the **`Systems`** tab, followed by the **`Kickstart`** subtab in the left navigation bar.
2. On the **`Kickstart Overview`** page, click the **`Create a New Kickstart Profile`** link in the **`Kickstart Actions`** widget in the upper right corner.
3. You should now find yourself on Step 1 of the kickstart profile creation process:
    a. Enter a label for your profile that will enable you to distinguish it from your other profiles. For the remaining instructions, we'll assume the label is **`host-system-for-virtual-guests`**.
    b. For the **`Base Channel`** field, select Red Hat Enterprise Linux (v.5 for $ARCH) (where $ARCH is the architecture of your host system.

Note

You may install 32-bit Red Hat Enterprise Linux 5 on a 64-bit host system. If you choose to do this, however, please be aware that your guest systems must also run the 32-bit version of Red Hat Enterprise Linux.

    c. In the **`Kickstartable Tree`** field, select **`ks-rhel-$ARCH-server-5`** where $ARCH is the architecture of your host system.
    d. Please select **`Para-Virtualized Host`** for the **`Virtualization Type`** field.
    e. Finally, click the **`Next`** button in the lower right of the screen to continue on to the next step.

Note

If any of the fields are missing the options indicated above, you may not have successfully synced software channel content to your Satellite from Red Hat's servers. Please review the *Red hat Network Satellite 5.0.0 Guide* for information on syncing software content to your Satellite.

4. For Step 2 of the kickstart profile creation process, select the location of the distribution files for the installation of your host system. There should already be a **Default Download Location** filled out and selected for you on this screen. Click the **Next** button on this screen to continue to Step 3.

Note

As in the previous step, if the default download location is missing, you may not have successfully synced software channel content to your Satellite from Red Hat's server.

5. For Step 3 of the kickstart profile creation process, please choose a root password to set on the host system you will be provisioning, and click **Next** to finish creation of the profile.
6. This completes kickstart profile creation. After completing Step 3, you are taken to the newly-created kickstart profile. You may browse through the various tabs of the profile and modify the settings as you see fit, but this is not necessary as the default settings should work well for the majority of cases.

8.1.2. Kickstart Your Host System

Next, kickstart your host system using your newly-created kickstart profile. There are three different scenarios for kickstarting your host system. Please read through these three scenarios below, and follow the instructions for the scenario that applies best to you:

8.1.2.1. Your Host System Has Red Hat Enterprise Linux 4 or Earlier Installed

In this case, register your host system to your Satellite and schedule the kickstart process via the Satellite's web interface.

1. First, register your host system to your Satellite. Use **ssh** to connect to your host system. Register your host system to your satellite issuing the following command as root:

```
rhnreg_ks
--serverUrl=htt://your-satellite.example.com/XMLRPC \
--username=username --password=password
```

Note

If your host system is already registered to a different Red Hat Network server, asdd the **--force** option to the command above.

2. Next, open up the host system's profile in the Satellite web interface. Log into the web interface of your Satellite at https://your-satellite.example.com/. Click on the **Systems** tab in the top red

navigation bar. You should see the host system you just registered — click on its profile name to access its system profile page.

3. Add a provisioning entitlement to your host system. From your host system profile page, click on **Details** ⇒ **Properties** tab. Check the **Provisioning** checkbox in the **Add-On Entitlements** field, and click the **Update Properties** button in the lower right hand corner of the screen.
4. Next, schedule the kickstart. You are brought back to the host system's profile page. You should now see a **Provisioning** tab in the system profile. Click on this tab. This should bring up the **Schedule Kickstart** page for the system.
5. Select the kickstart profile we created for this host earlier. Then, select the **Schedule Kickstart and Finish** button in the lower right-hand corner of the screen.

Note

If you do not see the kickstart profile you created earlier on the host system's **Schedule Kickstart** page, you may have created a kickstart profile for an architecture that does not match the architecture of the host system you have registered. If this is the case, open the kickstart profile by navigating to **Systems** ⇒ **Kickstart** ⇒ **Profiles** within the Satellite web interface, and clicking on the label for the host system's kickstart profile. Click on the **Kickstart Detail** ⇒ **Operating System** tab, and select items under the **Base Channel** and **Available Trees** selections that match the architecture of your host system. Click on the **Update Kickstart** button in the lower right hand corner of the screen, and navigate back to the host system's **Schedule Kickstart** page, following the steps above this note.

6. After scheduling the kickstart, you will be taken to a **Kickstart Status** screen in the Satellite's web interface. Keep your web browser open to that page to follow along with the host system's progress.
7. Use **ssh** to connect to the host system, and run the command **rhn_check**. This should cause the kickstart process to behind immediately rather than the next time the **rhn_check** process runs on the system. You should immediately see output indicating the start of a kickstart process on the host system, and it will eventually warn you that the system is going dow for reboot in three minutes.
8. After three minutes have passed, the system will reboot. Follow the progress of the kickstart via the Satellite web interface.
9. Depending on various factors, the kickstart process may take between ten and thirty minutes. At the end of this time period, the Satellite kickstart status page should indicate if the kickstart finished successfully.

Tip

If the kickstart fails, the Satellite kickstart status page should indicate that there was a failure. For more details on why the kickstart failed, click on the **Events** ⇒ **History** tab in the host system's profile, and click on the name of the kickstart event that failed to get more details on the failure. It may also be useful to consult **/var/log/up2date** on the host system for troubleshooting purposes.

8.1.2.2. You Host System Does Not have Red Hat Enterprise Linux Installed

First, create a boot CD to initiate the kickstart on your host system. You will be able to use the kickstart profile we created in earlier steps to provision the host. Note you must have physical access to the machine you intend to use in order to follow these steps:

1. You will find an ISO to create a boot CD for you host by using **ssh** to log into your Satellite. It is at the following location on your satellite:

   ```
   /var/satellite/rhn/kickstart/ks-rhel-i386-server-5/images/boot.iso
   ```

   For details on how to use this ISO image to burn a CD using Linux, please refer to the following Red Hat Knowledgebase Article:

   http://kbase.redhat.com/faq/FAQ_80_446.shtm

   If you must burn this ISO image to CD using another operating system, please refer to the following Knowledgebase Article:

   http://kbase.redhat.com/faq/FAQ_35_1897.shtm

   Tip

   It is possible to use a flash-memory USB key to boot your system in order to kickstart it. Refer to the *Red Hat Enterprise Linux System Administration Guide* (available at http://www.redhat.com/docs/manuals/enterprise/) for tips on how to do this. Note that your host system's hardware must support boot via these devices.

2. Insert the boot CD in the drive and reboot the system, making sure the CD-ROM drive is set as the primary boot device in the system's' BIOS.
3. After reboot, you should find yourself at a boot prompt. Type the following command at this prompt to start your kickstart:

   ```
   linux \
   ks=http://your-satellite.example.com/iskcstart/ks/label/the profile label you created earlier
   ```

   Note

   For some systems you may either need to add **ksdevice=eth0** to the command above or disable one of two or more NICs in the system's BIOS to avoid confusion during the kickstart process.

4. The kickstart for your host system should begin. It should take around fifteen minutes to complete. Upon successful completion of this kickstart, you will have provisioned a host system for your virtual guest and registered it to you Satellite.

8.1.2.3. Your Host System Has Red Hat Enterprise Linux 5 Installed

You should register your host system to your Satellite and check to see if the required **xen** packages are installed on the system. If they are not, install them using the Satellite

1. Fist, register your host system to your Satellite. Use **ssh** to connect to your host system. Register your host system to your satellite issuing the following command as root:

```
rhnref_ks --serverUrl=http://your-satellite.example.com/XMLRPC \
--username=username --password=password
```

Note

If your host system is already registered to a different Red Hat Network server, add the **--force** to the command above.

2. Next, open up the host system's profile in the Satellite web interface. Log into the web interface of your Satellite at https://your-satellite.example.com/. Click on the **Systems** tab in the top red navigational bar. You should see the host system you just registered - click on its profile name to access its system profile page.
3. Make sure your system has access to the software channels it needs to access the software required for hosting virtual guests. From your host system's profile page, click on the **Alter Channel Subscriptions** link in the upper right side of the profile page under the **Subscribed Channels** header. Check the **RHEL Virtualization** and **Red Hat Network Tools for RHEL Server** checkboxes and click the **Change Subscriptions** button underneath the list of channels.
4. Next, check to see if you have the necessary software installed for hosting virtual guest on the system. On the host system, issue the following command as root:

   ```
   rpm -q xen kernel-xen rhn-virtualization-host
   ```

   If **rpm** indicates these packages are not installed, you must install them by running the following command as root on the system:

   ```
   yum install dxen kernel-xen rhn-virtualization-host
   ```

   You will then need to edit the **/etc/grub.conf** configuration file to boot the new xen kernel by default. To do this, select the lines in **grub.conf** that pertain to the xen kernel from the beginning of the **title** line to the end of the **initrd** line, copy the lines, delete them, and paste them so they are the first kernel entry in **grub.conf**. Also ensure that the value of the default variable at the top of **grub.conf** is set to a value of '0'.
5. Reboot the system, boot it into the xen kernel. The system should not automatically boot into the xen kernel on reboot but if you would like to make sure it has for troubleshooting purposes, use the command **uname -r** to see if the running kernel is a xen kernel. If you do not see the **xen** string in the name of the kernel, you have not booted into the correct kernel.

   Note

   If the system already has **xen** and **kernel-xen** installed you do not need to reboot after installing **rhn-virtualization-host**.

6. You will also need to install and run the **osad** package in order for your host system to be responsive to commands sent from the Satellite, such as start, pause, resume, and shutdown. To install:

```
yum install -y osad
```

after installation, you should then start the **osad** process:

```
/sbin/service osad restart
```

7. Your host system should now be ready for RHN virtual guest provisioning.

8.2. Setting Up Your Virtual Systems

In order to work with virtual guest systems, you must first create a kickstart profile that will allow you to easily provision virtual guests, then you must provision the guests.

8.2.1. Create a Kickstart Profile for the Guest Systems

1. Log on to the Satellite's web interface. Navigate to the **Kickstart Overview** screen by clicking on the **Manage Kickstarts** link in the **Tasks** widget in **Your RHN**, or by clicking on **Systems** in the top navigation bar ⇒ **Kickstart** from the left navigation bar.
2. On the **Kickstart Overview** page, click the **Create a new Kickstart Profile** link in the **Kickstart Actions** widget in the upper right corner.
3. The next page displayed is Step 1 of the kickstart profile creation process:
    a. Enter a label for the profile that will allow you to distinguish it from the other profiles. A good choice would be **guest-system**.
    b. For the **Base Channel** field, select **Red Hat Enterprise Linux $PRODUCT (v.5 for $ARCH)** where $ARCH is the architecture of your host system's operating system and $PRODUCT is either Server or Client.

Note

Red Hat Enterprise Linux Client 5 may not be available for selection if you did not sync the Client software channels to your Satellite.

Tip

Please note that the channel labels for Red Hat Enterprise Linux 5 and Red Hat Enterprise Linux 5 Desktop refer to 'server' and 'client' respectively.

    c. For the **Kickstartable Tree** field, you should select **ks-rhel-$ARCH-$PRODUCT-5** where $ARCH is the architecture of your host system and $PRODUCT is either 'server' or 'client', depending on which product with which you would like to provision your guest.
    d. Select **Para-Virtualized Guest** for the **Virtualization Type** field.
    e. Finally, click the **Next** button in the lower right of the screen to continue on to the next step.
4. For Step 2 of the kickstart profile creation process, select the location of the distribution files for the installation of your guest system. There should already be a **Default Download Location** filled out and selected for you on this screen. Click the **Next** button on this screen to continue to Step 3.

Note

As in the previous step, if the default download location is missing, you may not have successfully synced software channel content to your Satellite from Red Hat's servers.

5. For Step 3 of the kickstart profile creation process, choose a root password for the guest system you are provisioning, and click **Next** to finish creation of the profile.
6. This completes kickstart profile creation. After completing Step 3 you should be taken to the profile details. You may browse through the various tabs of the profile and modify the settings as you see fit, but this is not necessary as the default settings should work well for the majority of cases. While the interface allows you to allocate less, we strongly recommend allocating at least 2 GB of storage for your guest system with this kickstart profile.

8.2.2. Provision Your Guest Systems

1. Log into the Satellite's web interface. Browse to your host system's profile by clicking on the **Systems** tab in the top navigation bar, and click on the system's name.
2. To schedule a kickstart for a guest system, go to the **Virtualization** ⇒ **Provisioning** tab in the host system's profile. For the **Guest Name** field choose **guest1**. For the **Memory Allocation**, **Virtual CPUs**, and **Storage** fields, the default values should be fine. Feel free to change these as desired, taking note of the advice provided for each field in the interface. For the **Kickstart Profile** field, select the guest system profile we created in the last step.
3. Finally, click on the **Schedule Kickstart and Finish** button in the lower-right corner of the screen. You will be taken to the **Kickstart Status** page where you can follow along with the guest's kickstart progress. After ten to fifteen minutes the status screen should indicate the kickstart successfully completed. To view your new guest, click on the **Virtualization** tab of the host system's profile on the Satellite. To view a list of virtual host systems indicating which guest systems are hosted on each, navigate to **Systems** ⇒ **Systems** ⇒ **Virtual Systems**.

Note

If you do not see the **Initiate a kickstart for a Xen** guest message on the **Kickstart Status** page shortly after scheduling the kickstart of the guest, you may be missing **osad** on your host.
Host systems require the **osad** package in order to be responsive to commands sent from the Satellite, such as start, pause, resume, and shutdown. If **osad** is not installed and running, the host system will not receive these commands from the web interface for 2.5 hours, or the next time that the RHN daemon runds.
You can check whether or not **osad** is installing and running by checking the **OSA Status** field in the host system's profile on the Satellite. If the field does not exist or indicates a failure of that the system has not contact Satellite in several minutes, then you will need to install **yum** (using the command **yum install -y osad**) before you can successfully provision a guest on the host.

Tip

You may receive the following message from the **Kickstart Status** page during the guest's kickstart:
The install process on the guest system has not communicated to RHN in the past n minutes. This may be due to a hung install process, or it may just be due to a slow install because of hardware constraints. A log of the installation process is available, you may wish to review it to troubleshoot this issue.
Be patient and do not worry if you see this message unless more than twenty minutes have pased. To check if the kickstart is continuing, check the installation log to make sure there are no errors, and as you reload the Kickstart Status page check to see that the Last File Request field continues to be updated.

4. If you would like to register additional guests to your host, repeat the steps above. It is important to remember that you can only provision one guest at a time. If you attempt to schedule a guest kickstart while another is currently taking place, the current guest kickstart process will be canceled and the new guest kickstart process will begin.
5. View your newly-created virtual guest's system in the Satellite's web interface by clicking on the **Virtualization** tab in the host system's profile. Then, click on the profile name of your virtual system. You will be brought to its Satellite system profile.

8.3. Working With Your Virtual Systems

8.3.1. Logging into Virtual Systems Directly via SSH

1. You will need to locate the virtual system's IP address. Locate it by navigating to the **Systems** ⇒ **Virtual Systems** tab and clicking on the virtual system's profile name.
2. On the virtual system's profile page, you'll find the IP address in the left-hand informational column in the **IP Address** field.
3. Connect to the IP address by using **ssh** as root, using the password you set for the virtual system in the kickstart profile you created for it earlier.

8.3.2. Gaining Console Access Via the Host

1. First you will need to connect to the host system and determine the ID number of the guest you would like to work with. Connect to the host system via **ssh** and run the following command:

   ```
   xm list
   ```

   This should provide you with a list all of the guests you created on your Satellite, including their ID number. look for the guest, **guest1**, that we created earlier in this list. If, for example, this guest has been assigned an ID of 2, then:
2. Run the following command to access the console of this virtual system:

   ```
   xm console 2
   ```

   You should immediately be able to view a login prompt on **guest1**.

3. Login to **guest1** as root using the same password you set in the kickstart profile you used to provision the system.

   (There may be some messages on the screen. In this case, hit the **Enter** key on your keyboard to receive a fresh login prompt.)
4. To exit the guest console and return to the host system's command prompt, you may hit the **Ctrl** and **]** keys on your keyboard simultaneously.

8.3.3. Installing Software Via the Satellite Web Interface

1. Browse to the virtual system's profile in your Satellite's web interface by logging in and navigating to **Systems** ⇒ **Systems** ⇒ **Virtual Systems** and clicking on the name of your virtual system's profile.
2. In the virtual system's profile, click on the **Software** ⇒ **Packages** tab.
3. Click on **Install New Packages** in the **Packages** tab menu.
4. Select the packages you wish to install and click the **Install Selected Packages** button in the lower right-hand corner of the screen.
5. Review the package install details and click on the **Confirm** button in the lower right-hand corner of the screen.
6. The package install will take place the next time the guest system checks in with the Satellite. To force the install to take place immediately, you may run the **rhn_check** command on the guest system.

8.3.4. Installing Software Via Yum From the Virtual System

Your virtual system registered to your Satellite as part of the guest provisioning process, so you may simply use the **yum** command to install and update software. For example, to install the text editor vim, issue the following command:

```
yum install -y vim-enhanced
```

8.3.5. Deleting Virtual Systems

Deleting a virtual system is a multi-step process.

1. First you must shut down the virtual system that you wish to delete. You may do this by browsing to the host system's profile in the Satellite web interface, clicking on the virtualization tab, and checking off the virtual systems that you would like to delete. Finish shutting down by clicking the **Shutdown Systems** button at the bottom of the screen.
2. Next, delete the virtual system from Satellite. This is accomplished by checking off the virtual system's checkbox and clicking the **Delete System** button at the bottom of the screen>

Tip

Please allow for at least two minutes between shutting down a virtual system and deleting it. Otherwise, the virtual system may not shut down properly and you will delete it while it is running. If you delete a virtual system from Satellite while it is running, it will reappear on the Satellite the next time it checks in. If this happens, simply shutdown the system, wait two minutes, and delete it again.

3. Delete the disk image for the virtual system you would like to delete. You will find the disk image for **guest1**, for example, at the following location on the host system:

```
/var/lib/xen/disk-images/guest1.disk
```

   Delete it with the following command:

```
rm /var/lib/xen/disk-images/guest1.disk
```

4. Finally, you must delete the RHN configuration files from the host system. To locate the RHN configuration file for **guest1**, run the following command:

```
grep guest1 /etc/sysconfig/rhn/virt/*.xml
```

   Then delete the file indicated. For example:

```
rm /etc/sysconfig/rhn/virt/14e5cfbf72342515236ad74b260c2f6b.xml
```

5. You have successfully deleted a guest system from your host system and from Satellite.

Chapter 9. UNIX Support Guide

9.1. Introduction

This chapter documents the installation procedure for, and identifies differences in, Red Hat Network functionality when used to manage UNIX-based client systems. RHN offers UNIX support to help customers migrate from UNIX to Linux. Because of the limited scope of this task, the features offered for UNIX client management are not as comprehensive as those available for managing Red Hat Enterprise Linux systems.

Subsequent sections specify supported UNIX variants, RHN features supported by the UNIX management system, the prerequisites for managing a UNIX system with RHN, as well as the installation procedure for UNIX clients.

9.1.1. Supported UNIX Variants

The following UNIX variants, versions, and architectures are supported by Red Hat Network:

- Solaris 8, 9, 10 (sparc)
- Solaris 9, 10 (x86)

9.1.2. Prerequisites

These items are needed to obtain UNIX support:

- RHN Satellite 5.0.0 or later
- A Satellite certificate with Management entitlements
- Management entitlements for each UNIX client
- RHN packages for UNIX including python, pyOpenSSL, and the Red Hat Network Client packages.
- Sunfreeware packages that provide supporting libraries. Some of these packages are available via the RHN Satellite. Refer to Section 9.3.1, “Download and Install Additional Packages” for the complete list.

9.1.3. Included Features

The following features are included in the UNIX support service level as they exist within RHN:

- The **Red Hat Network Service Daemon** (**`rhnsd`**), which triggers **`rhn_check`** according to a configurable interval
- The **Red Hat Network Configuration Client** (**`rhncfg-client`**), which executes all configuration actions scheduled from the Satellite
- The **Red Hat Network Configuration Manager** (**`rhncfg-manager`**), which allows command line administration of RHN configuration channels
- The **`rhn_check`** program, which checks in with the Satellite and performs any actions scheduled from the server
- All Management-level functionality, such as system grouping, package profile comparison, and use of the System Set Manager to administer multiple systems at once
- A Provisioning feature called *Remote Command* that enables users to schedule root-level commands on any managed client through the Satellite's website, if the client allows this action

9.1.4. Differences in Functionality

The following RHN features work differently in a UNIX environment:

- The **Red Hat Update Agent for UNIX** offers a much smaller set of options than its Linux counterpart and relies upon the operating system's native toolset for package installation, rather than **`rpm`** - Refer to Section 9.4.2.3, “Updating From the Command Line” for the precise list of options.
- The **RHN Push** application has been similarly modified to upload native UNIX file types, including packages, patches, and patch clusters.

  Since Solaris package, patch and patch cluster files are different from RPM files, the channel upload mechanism is somewhat different.There are two applications in the **`rhnpush`** package for Solaris:
  - The first, **`solaris2mpm`**, is an RHN utility that create an MPM file for each Solaris package or patch. The neutral format of the MPM file allows the Satellite to understand and manage the uploaded files.
  - The second, **`rhnpush`**, has been extended so that it can handle MOM as well as RPM files. Otherwise, it operates identically to the Linux version of **`rhnpush`**.
- The **`Channels`** tab of the RHN website has been augmented to accommodate the storage and installation of native UNIX file types.

9.1.5. Excluded Features

The following RHN features are not available with the UNIX support system:

- All Provisioning-level functionality, such as kickstarting and package rollback, with the exception of configuration file management
- All Errata-related options, since the concept of Errata Updates is not understood in UNIX
- Source files for packages

In addition, *answer* files are not yet supported. Support for such files is planned for a future release.

9.2. Satellite Server Preparation/Configuration

You must configure the Satellite to support UNIX clients before the required files are available for deployment to the client systems. This can be accomplished in one of two ways, depending on whether you have yet installed your Satellite server:

1. During the Satellite installation:

   Enable UNIX support on the Satellite by checking the "Enable Solaris Support" box during the installation process, as pictured:

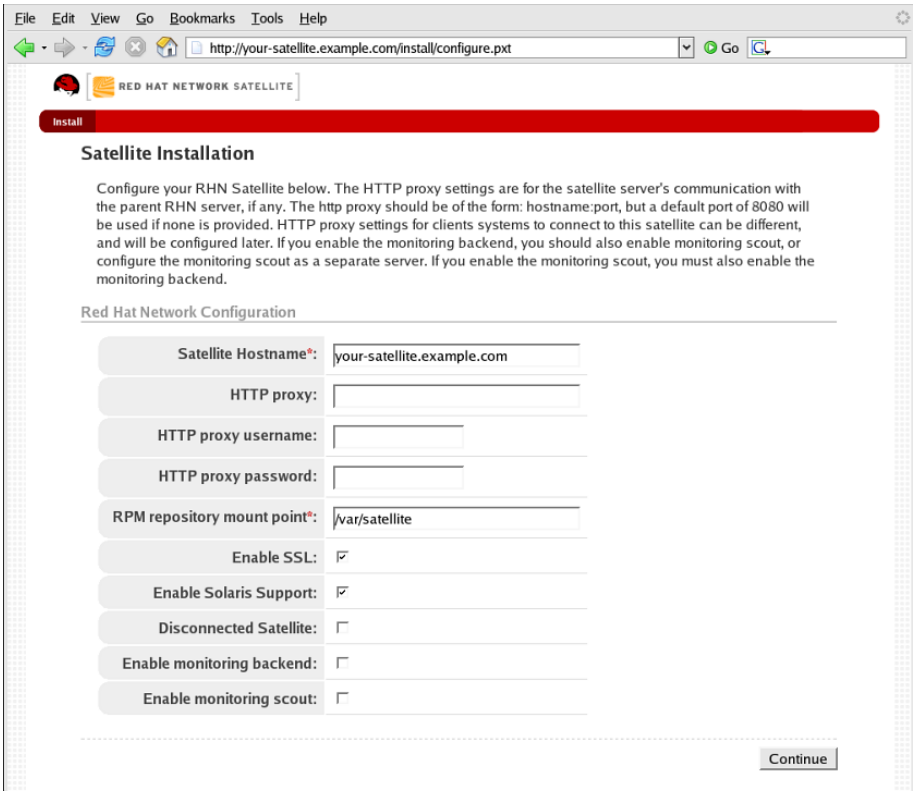

File Edit View Go Bookmarks Tools Help
http://your-satellite.example.com/install/configure.pxt
Go
RED HAT NETWORK SATELLITE
Install
Satellite Installation
Configure your RHN Satellite below. The HTTP proxy settings are for the satellite server's communication with the parent RHN server, if any. The http proxy should be of the form: hostname:port, but a default port of 8080 will be used if none is provided. HTTP proxy settings for clients systems to connect to this satellite can be different, and will be configured later. If you enable the monitoring backend, you should also enable monitoring scout, or configure the monitoring scout as a separate server. If you enable the monitoring scout, you must also enable the monitoring backend.
Red Hat Network Configuration
Satellite Hostname*:
your-satellite.example.com
HTTP proxy:
HTTP proxy username:
HTTP proxy password:
RPM repository mount point*:
/var/satellite
Enable SSL:
Enable Solaris Support:
Disconnected Satellite:
Enable monitoring backend:
Enable monitoring scout:
Continue

Figure 9.1. Enabling UNIX Support During Satellite Installation

2. After the Satellite has been installed:

   Enable UNIX support by configuring the Satellite after it has been installed. To do so, select **Satellite Tools** in the top menubar, then select **Satellite Configuration** in the left navigation bar. In the screen that follows, check the **`Enable Solaris Support`** box, as pictured:

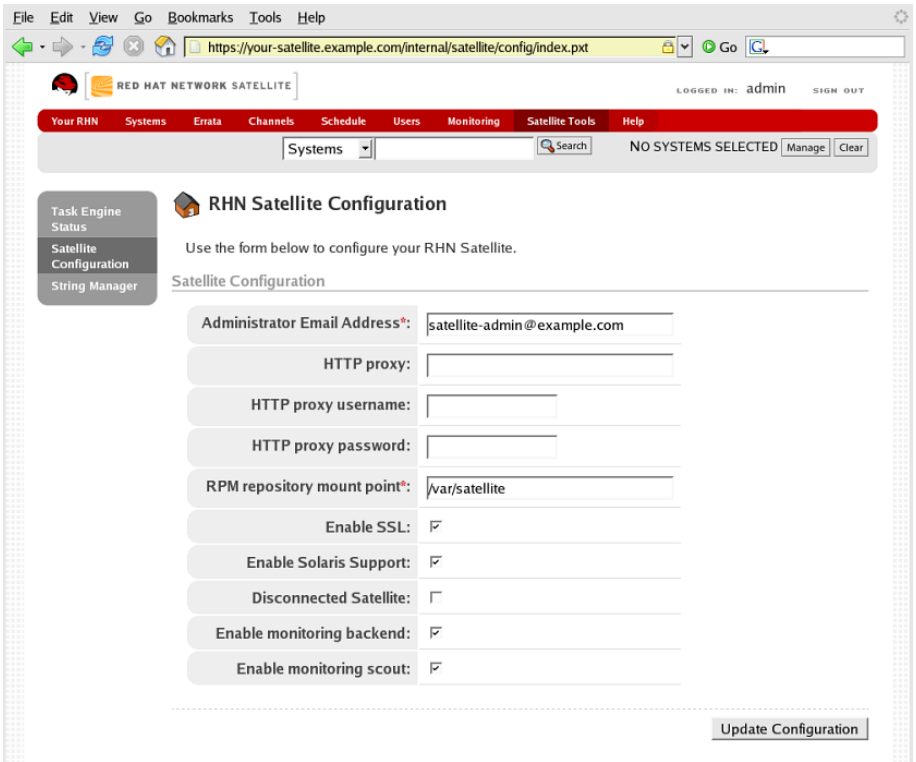


Figure 9.2. Enabling UNIX Support After Satellite Installation

Click the **Update Configuration** button to confirm the change.

3. Finally, you must create a base channel to which your client systems may subscribe. This is because RHN does not provide UNIX content; as a result, you cannot use **satellite-sync** to create the channel.

   To create a Solaris channel, login to the web interface of the Satellite as either an Organization Administrator or a certificate authority. Navigate to the **Channel** tab, followed by the **Manage Software Channels** from the left navigation bar. Click the **create new channel** link in the upper right of the resulting screen. Provide a name and label for your new channel, and select either **Sparc Solaris** or **i386 Solaris** as the architecture, depending on the architecture of your client.

9.3. Client System Preparation

Before your UNIX-based client systems benefit from Red Hat Network, they must be prepared for connection:

1. Download and install **gzip** and required third-party libraries.
2. Download the RHN application tarball from the Satellite to the client and install the contents.
3. Next, deploy the SSL certificates required for a secure connection.
4. Configure the client applications to connect to the RHN Satellite.

Once finished, your systems will be ready to begin receiving RHN updates. The following three section explain these steps in detail.

9.3.1. Download and Install Additional Packages

This section steps you through the process of downloading and installing third-party applications and the RHN applications from the Satellite onto the UNIX client.

Of primary importance is the **Red Hat Update Agent for UNIX** (**up2date**), which provides the link between your client systems and Red Hat Network. The UNIX-specific version of the **Red Hat Update Agent** is limited in functionality compared to its Linux counterpart but still enables system registration and facilitates package installs and patches. Refer to Section 9.4, “Registration and Updates” for a full description of the tool's options.

Note

It may be useful to enter the command **bash** when first logging into the Solaris client. If the BASH shell is available, it will make the system's behavior as Linux-like as possible.

9.3.1.1. Install Third-Party Packages

Installation of the RHN applications cannot proceed unless the following utility and libraries are present:

- **gzip**
- **libgcc**
- **openssl**
- **zlib**

The **gzip** utility is provided by the SUNWgzip package and may be downloaded from http://www.sunfreeware.com.

On recent versions of Solaris, the necessary libraries are provided by the following natively installed packages:

- **SUNWgccruntime**
- **SUNWopenssl***
- **SUNWzlib**

For older Solaris versions, the following required packages may be downloaded from http://www.sunfreeware.com:

- **SMClibgcc** or **SMCgcc**
- **SMCossl**
- **SMCzlib**

To verify if a package is installed on the client, use the **pkginfo** command. For example, to check for a package that contains "zlib" in the name, run the following command:

```
# pkginfo | grep zlib
```

Note

Solaris package archive names differ from the name of the installed package. For example, the package archive **libgcc<version>-sol<solaris-version>-sparc-local.gz** becomes SMClibgcc after installation

9.3.1.2. Configure the Library Search Path

In order to allow the Solaris client to use the libraries installed in the previous step, you must add their location to the library search path. To do so, first check the current library search path":

```
# crle -c /var/ld/ld.config
```

Make a note of the current Default Library Path. Next, modify the path to also include the components shown below. Note that the **-l** option resets the value, rather than appending it, so if there already were values set on your system, prepend them to the -l parameter.

On sparc:

```
 # crle -c /var/ld/ld.config -l /other/existing/path:/lib:/usr/lib:/usr/local/lib
```

On x86:

```
# crle -c /var/ld/ld.config -l
/other/existing/path:/lib:/usr/lib:/usr/local/lib:/usr/sfw/lib
```

9.3.1.3. Download RHN Client Packages

Download the appropriate tarball of packages from the **/var/www/html/pub/** directory of your

Satellite. If you are able to use a GUI web browser like Mozilla, navigate to the **/pub** directory of the Satellite and save the appropriate tarball to your client:

```
http://your-satellite.example.com/pub/rhn-solaris-bootstrap-<version>-<solaris-arch>-<solaris-version>.tar.gz
```

If you must download the tarball from the command line, it should be possible to use **ftp** to transfer the file from the Satellite to the client.

Using **gzip**, decompress the tarball. You should have the following packages:

- **RHATpossl**
- **RHATrcfg**
- **RHATrcfga**
- **RHATrcfgc**
- **THATrcfgm**
- **RHATrhnc**
- **RHATrhnl**
- **RHATrpush**
- **RHATsmart**

SMClibgcc and **SMCosslg** may also be included in the tarball.

9.3.1.4. Install the RHN Packages

Change to the uncompressed directory and use the UNIX variant's native installation tool to install each package. For example, on Solaris, use the **pkgadd** command. Answer "yes" to any prompts during package install.

Here is how a typical installation might proceed:

```
# pkgadd -d RHATpossl-0.6-1.p24.6.pkg all
# pkgadd -d RHATpythn-2.4.1-2.rhn.4.sol9.pkg all
# pkgadd -d RHATrhnl-1.8-7.p23.pkg all
...
```

Note

You may choose to use the **-n** of **pkgadd**, which runs the command in non-interactive mode. However, this may cause the installation of some packages to fail silently on Solaris 10.

Continue until each package is installed in the RHN-specific path: **/opt/redhat/rhn/solaris/**.

9.3.1.5. Include RHN Packages in the PATH

In order to make the RHN packages available at each login, you may wish to add them to your PATH. To do so, add these commands to your login script:

```
# PATH=$PATH:/opt/redhat/rhn/solaris/bin
# PATH=$PATH:/opt/redhat/rhn/solaris/usr/bin
# PATH=$PATH:/opt/redhat/rhn/solaris/usr/sbin
# export PATH
```

To enable access to the RHN client command man pages, add them to your MANPATH. To do so, add the following commands to your login script:

```
# MANPATH=$MANPATH:/opt/redhat/rhn/solaris/man
# export MANPATH
```

Alternatively, you can also access the man pages from the command line, with the following command:

```
# man -M /opt/redhat/rhn/solaris/man <man page>
```

Finally, add the Red Hat Libraries to your PATH as you did with **libgcc**, **openssl** and **zlib**.

```
crle -c /var/ld/ld.config -l <current library paths>:/opt/redhat/rhn/solaris/lib
```

9.3.2. Deploying Client SSL Certificates

To ensure secure data transfer, Red Hat strongly recommends the use of SSL. The RHN Satellite eases implementation of SSL by generating the necessary certificates during its installation. The server-side certificate is automatically installed on the Satellite itself, while the client certificate is placed in the **/pub/** directory of the Satellite's Web server.

To install the certificate, follow these steps for each client:

1. Download the SSL certificate from the **/var/www/html/pub/** directory of the RHN Satellite onto the client system. The certificate will be named something similar to **RHN-ORG-TRUSTED-SSL-CERT**. It is accessible via the web at the following URL: **https://your-satellite.example.com/pub/RHN-ORG-TRUSTED-SSL-CERT**.
2. Move the client SSL certificate to the RHN-specific directory for your UNIX variant. For Solaris, this can be accomplished with a command similar to:

   ```
   mv /path/to/RHN-ORG-TRUSTED-SSL-CERT
   /opt/redhat/rhn/solaris/usr/share/rhn/
   ```

When finished, the new client certificate will be installed in the appropriate directory for your UNIX system. If you have a large number of systems to prepare for RHN management, you may script this entire process.

Now you must reconfigure the RHN client applications to refer to the newly installed SSL certificate. Refer to Section 9.3.3, “Configuring the clients” for instructions.

9.3.3. Configuring the clients

The final step before registering your client systems with Red Hat Network is to reconfigure their RHN applications to use the new SSL certificate and obtain updates from the RHN Satellite. Both of these changes can be made by editing the configuration file of the **Red Hat Update Agent**, which provides registration and update functionality.

Follow these steps on each client system:

1. As root, change to the RHN configuration directory for the system. For Solaris, the full path is **/opt/redhat/rhn/solaris/etc/sysconfig/rhn/**.
2. Open the **up2date** configuration file in a text editor.
3. Find the ***serverURL*** entry and set its value to the fully qualified domain name (FQDN) of your RHN Satellite:

```
serverURL[comment]=Remote server URL
serverURL=https://your-satellite.example.com/XMLRPC
```

4. Ensure the application refers to the RHN Satellite even when SSL is turned off by also setting the ***noSSLServerURL*** value to the Satellite:

```
noSSLServerURL[comment]=Remote server URL without SSL
noSSLServerURL=http://your-satellite.example.com/XMLRPC
```

5. With the **up2date** configuration file still open, find the ***sslCACert*** entry and set its value to the name and location of the SSL certificate described in Section 9.3.2, “Deploying Client SSL Certificates”, for example:

```
sslCACert[comment]=The CA cert used to verify the ssl server
sslCACert=/opt/redhat/rhn/solaris/usr/share/rhn/RHN-ORG-TRUSTED-SSL-CERT
```

Your client systems are now ready for registration with Red Hat Network and management by your Satellite.

9.4. Registration and Updates

Now that you have installed RHN-specific packages, implemented SSL, and reconfigured your client systems to connect to the RHN Satellite, you are ready to begin registering systems and obtaining updates.

9.4.1. Registering Systems

This section describes the RHN registration process for UNIX systems. You must use the **rhnreg_ks** command to accomplish this; the use of activation keys for registering your systems is optional. These keys allow you to predetermine settings within RHN, such as base channels and system groups, and to apply those automatically to systems during their registration.

Since activation key generation and use is covered extensively in other chapters, this section focuses on differences when applying them to UNIX variants. Refer to Section 6.4.6.1, “Managing Activation Keys” for full descriptions of this process.

To register UNIX systems with your RHN Satellite, accomplish the following tasks in this order:

1. Log into the Satellite's web interface and click the **Systems** tab in the top navigation bar followed by **Activation Keys** in the left navigation bar. Then click the **create new key** link at the top-right corner of the page.
2. On the following page, select the base channel you created at the end of Section 9.2, “Satellite Server Preparation/Configuration”.

3. After creating the key, click its name in the **Activation Keys** list to enhance its RHN settings by associating software and configuration channels and system groups.
4. Open a terminal on the client system to be registered and switch user to root.
5. Use **rhnreg_ks** along with the **--activationkey** option to register the client with the Satellite. The string of characters that make up the key may be copied directly from the **Activation Keys** list on the website. The resulting command will look something like the following:

```
rhnreg_ks --activationkey=b25fef0966659314ef9156786bd9f3af
```

6. Go back to the website, click the name of the activation key, and ensure the new system appears within the **Activated Systems** tab.

9.4.2. Obtaining Updates

Package updates in UNIX are handled much differently than in Linux. For instance, Solaris relies on Patch Clusters to update multiple packages at once, while Red Hat operating systems use Errata Updates to associate upgrades with specific packages. In addition, Solaris uses answer files to automate interactive package installations, something Linux doesn't understand, while Red Hat offers the concept of source packages. For this reason, this section seeks to highlight differences in using RHN tools on UNIX systems. (Note: RHN does not support Solaris answer files in the current release; such support is planned for future releases.)

Despite inherent differences, such as the lack of Errata, the channel and package management interfaces within the RHN website on the Satellite work largely the same for UNIX systems. All software channels designed to serve UNIX variants can be constructed almost exactly as the custom channels described in the *RHN Channel Management Guide*. The most significant difference is the architecture. When creating a UNIX software channel, ensure you select the base channel architecture appropriate for the systems to be served.

Furthermore, Red Hat recommends you break down your packages into base and child channels depending on their nature. For example, on Solaris, installation packages should go in the Solaris base channel, while patches and Patch Clusters should go in a child channel of the Solaris base channel. Extra installation packages can go in a separate Extras child channel.

RHN treats patches similarly to packages; they are listed and installed in the same way and with the same interface as normal packages. Patches are 'numbered' by Solaris, and will have names like "patch-solaris-108434". The version of a Solaris patch is extracted from the original Solaris metadata, and the release is always 1.

Patch Clusters are bundles of patches that are installed as a unit. RHN keeps track of the last time that a Patch Cluster was installed successfully on a system. However, Patch Clusters are not tracked on the client as installed entities so they do not appear in the installed packages or patches list. Patch Cluster names look like "patch-cluster-solaris-7_Recommended". The version is a datestring, such as "20040206", the release is always 1 and the epoch is always 0.

9.4.2.1. Uploading Packages to the Satellite

RHN does not provide UNIX content; any Solaris packages, patches or Patch Clusters must be uploaded to the Satellite in a format that it understands from a client system. That package can then be managed and distributed to other systems. RHN created **solaris2mpm** to translate Solaris packages, patches, and patch clusters to a format that the Satellite can understand.

9.4.2.1.1. solaris2mpm

As mentioned briefly in Section 9.1.4, “Differences in Functionality”, **solaris2mpm** is part of RHN Push for Solaris. The content that is pushed to a Solaris channel on the Satellite must first be in .mpm format.

A .mpm file is an archive containing a description of the package data and the package or patch itself. The solaris2mpm command must be run on the client, never the Satellite.

Note

solaris2mpm requires free space equal to three times the size of any package, patch, or patch cluster it is converting. Normally, space in **/tmp/** will be used for this purpose. However, the **--tempdir** option allows you to specify another directory if necessary.

Multiple files may be specified on the command line of solaris2mpm. Below is a usage example:

```
# solaris2mpm RHATrpush-3.1.5-21.pkg RHATrpush-3.1.5-23.pkg
Opening archive, this may take a while
Writing out RHATrpush-3.1.5-21.sparc-solaris.mpm
Opening archive, this may take a while
Writing out RHATrpush-3.1.5-23.sparc-solaris.mpm
```

Because no other directory was specified, the resulting .mpm files are written to the /tmp/ directory. Note that the name of the resulting .mpm files includes the architecture of the client on which it was created. In this case, this was Sparc Solaris. The general format of mpm file names is:

```
name-version-release.arch.mpm
```

Patch clusters are "exploded" — .mpm files are generated for each patch in the cluster, as well as a top-level "meta" .mpm file containing information about the cluster as a whole.

Below are the options of solaris2mpm:

Table 9.1. solaris2mpm options

Option	Description
--version	Displays the program's version number and exits
-h, --help	Displays this information and exits
-?, --usage	Prints program usage information and exits
--tempdir=<tempdir>	Temporary directory to work from
--select-arch=<arch>	Selects the architecture (i386 or Sparc) for multi-arch packages.

9.4.2.1.2. rhnpush with .mpm Files

The Solaris version of **rhnpush** works like the standard utility, but with the added ability to handle .mpm files. Below is a usage example:

```
% rhnpush -v --server testbox.example.com --username myuser -c solaris-8 \
RHATrpush-3.1.5-*.mpm
 Red Hat Network password:
 Connecting to http://testbox.example.com/APP
 Uploading package RHATrpush-3.1.5-21.sparc-solaris.mpm
 Uploading package RHATrpush-3.1.5-23.sparc-solaris.mpm
```

Note

Patch cluster .mpm files must be pushed either concurrently with or after — never before — the .mpm files for the patches contained in that cluster.

Use solaris2mpm on each of the packages, patches, or patch clusters you wish to manage via the Satellite, then use RHN Push to upload them to the channel you created for them.

9.4.2.2. Updating Through the Website

To install packages or patches on an individual system, click the name of the system in the **Systems** category, select the packages from the Upgrade or Install lists of the **Packages** or **Patches** tab, and click **Install/Upgrade Selected Packages**.

To run a remote command while installing the package, click **Run Remote Command** rather than **Confirm**. Refer to Section 9.5, “Remote Commands” for instructions.

To install packages or patches on multiple systems at once, select the systems and click **System Set Manager** in the left navigation bar. Then, in the **Packages** tab, select the packages from the Upgrade or Install lists and click **Install/Upgrade Packages**. To complete the action, schedule the updates.

On Red Hat Enterprise Linux systems, the **rhnsd** daemon, which instructs the client system to check in with RHN, automatically starts at boot time. On Solaris systems, **rhnsd***does not* start at boot time by default. It can be started from the command line in this way:

```
rhnsd --foreground --interval=240
```

The default location for **rhnsd** is **/opt/redhat/rhn/solaris/usr/sbin/rhnsd**. Below are the available options for **rhnsd** on Solaris:

Table 9.2. rhnsd Options

Option	Description
-f, --foreground	Run in foreground
-i, --interval=MINS	Connect to Red Hat Network every MINS minutes
-v, --verbose	Log all actions to syslog
-h, --help	Give this help list
-u, --usage	Give this help list
-V, --version	Print program version

9.4.2.3. Updating From the Command Line

Like the website, command line use of the **Red Hat Update Agent** is affected by the limitations of UNIX package management. That said, most core functions can still be accomplished through the **up2date** command. The most significant difference is the absence of all options regarding source files. Refer to Table 9.3, "Update Agent Command Line Arguments" for the precise list of options available for UNIX systems.

The command line version of the **Red Hat Update Agent** accepts the following arguments on UNIX systems:

Table 9.3. Update Agent Command Line Arguments

Argument	Description
--version	Show program version information.
-h, **--help**	Show this help message and exit.
-v, **--verbose**	Show additional output.
-l, **--list**	List the latest versions of all packages installed.
-p, **--packages**	Update packages associated with this System Profile.
--hardware	Update this system's hardware profile on RHN.
--showall	List all packages available for download.
--show-available	List all the packages available that are not currently installed.
--show-orphans	List all the packages currently installed that are not in channels the system is subscribed to.
--show-channels	Show the channel names along with the package names where appropriate.
--installall	Install all available packages. Use with **--channel**.
--channel=*CHANNEL*	Specify which channels to update from using channel labels.
--get	Fetch the package specified without resolving dependencies.

9.5. Remote Commands

With UNIX support, RHN offers the flexibility of issuing remote commands on client systems through the Satellite's RHN website. This feature allows you to run virtually any (compatible) application or script on any system in your domain without ever having to open a terminal.

9.5.1. Enabling Commands

With the flexibility this tool offers comes great risk and the responsibility to mitigate that risk. For all practical purposes, this feature grants a root BASH prompt to anyone with administrative access to the system on the website.

This can be controlled, however, through the same config-enable mechanism used to determine which systems can have their configuration files managed by Red Hat Network. Refer to Section 6.4.2.9.3, "System Details ⇒ Configuration — " for details.

In short, you must create a directory and file on the UNIX system that tell RHN it is acceptable to run

remote commands on the machine. The directory must be named **script**, the file must be named **run**, and both must be located in the **/etc/sysconfig/rhn/allowed-actions/** directory specific to your UNIX variant.

For instance, in Solaris, issue this command to create the directory:

```
mkdir -p /opt/redhat/rhn/solaris/etc/sysconfig/rhn/allowed-actions/script
```

To create the requisite file in Solaris, issue this command:

```
touch /opt/redhat/rhn/solaris/etc/sysconfig/rhn/allowed-actions/script/run
```

9.5.2. Issuing Commands

You may schedule a remote command in a variety of ways: on an individual system, on multiple systems at once, and to accompany a package action.

To run a remote command on an individual system by itself, open the **System Details** page and click the **Remote Command** subtab. (Note that this subtab only appears if the system has a Provisioning entitlement.) On this page, establish the settings for the command. You may identify a specific user, group, and timeout period, as well as the script itself. Select a date and time to begin attempting the command, and click the **Schedule Remote Command** link.

Similarly, you may issue a remote command on multiple systems at once through the **System Set Manager**. Select the systems, go to the **System Set Manager**, click the **Misc** tab, and scroll down to the **Remote Command** section. From there you may run a remote command on the selected systems at once.

To run a remote command with a package action, schedule the action through the **Packages** tab of the **System Details** page and click **Run Remote Command** while confirming the action. Use the radio buttons at the top to determine whether the command should run before or after the package action, establish the settings for the command, and click **Schedule Package Install/Upgrade**.

Note that installing multiple packages that have different remote commands requires scheduling the installs separately or combining the commands into a single script.

Command Line Config Management Tools

In addition to the options provided in the RHN website, Red Hat Network offers two command line tools for managing a system's configuration files: the **Red Hat Network Configuration Client** and the **Red Hat Network Configuration Manager**. There is a complementary **Red Hat Network Actions Control** tool that is used to enable and disable configuration management on client systems. If you do not yet have these these tools installed, they can be found within the **`RHN Tools`** child channel for your operating system.

Tip

Keep in mind, whenever a configuration file is deployed via RHN, a backup of the previous file including its full path is made in the **`/var/lib/rhncfg/backups/`** directory on the affected system. The backup retains its filename but has a **`.rhn-cfg-backup`** extension appended.

A.1. Red Hat Network Actions Control

The **Red Hat Network Actions Control** (**`rhn-actions-control`**) application is used to enable and disable configuration management of a system. Client systems cannot be managed in this fashion by default. This tool allows Organization Administrators to enable or disable specific modes of allowable actions such as: *deploying* a configuration file onto the system, *uploading* a file from the system, *diffing* what is currently managed on a system and what is available, or allowing running arbitrary *remote commands*. These various modes are enabled/disabled by placing/removing files and directories in the **`/etc/sysconfig/rhn/allowed-actions/`** directory. Due to the default permissions on the **`/etc/sysconfig/rhn/`** directory, RHN Actions Control will most likely have to be run by someone with root access.

A.1.1. General command line options

There is a **`man`** page available, as there are for most command line tools, though the use of this tool is simple enough to describe here briefly. Simply decide what RHN scheduled actions should be enabled for use by system administrators. The following options enable the various scheduled action modes:

Table A.1. `rhn-actions-control` options

Option	Description
--enable-deploy	Allow rhncfg-client to deploy files.
--enable-diff	Allow rhncfg-client to diff files.
--enable-upload	Allow rhncfg-client to upload files.
--enable-mtime-upload	Allow rhncfg-client to upload mtime.
--enable-all	Allow rhncfg-client to do everything.
--enable-run	Enable script.run
--disable-deploy	Disable deployment.
--disable-diff	Disable diff
--disable-upload	Disable upload
--disable-mtime-upload	Disable mtime upload
--disable-all	Disable all options
--disable-run	Disable script.run
--report	Report whether the modes are enabled or disabled
-f, --force	Force the operation without asking first
-h, --help	show help message and exit

Once a mode is set — and for many, **`rhn-actions-control --enable-all`** is common — your system is now ready for config management through RHN.

A.2. Red Hat Network Configuration Client

As the name implies, the **Red Hat Network Configuration Client** (**`rhncfg-client`**) is installed and run from an individual client system. From there you may use it to gain knowledge about how RHN deploys configuration files to the client.

The **Red Hat Network Configuration Client** offers these primary modes: list, get, channels, diff, and verify.

A.2.1. Listing Config Files

To list the configuration files for the machine and the labels of the config channels containing them, issue the command:

```
rhncfg-client list
```

The output resembles the following list:

```
 Config Channel File config-channel-17 /etc/example-config.txt config-channel-
17 /var/spool/aalib.rpm config-channel-14 /etc/rhn/rhn.conf
```

These are the configuration files that apply to your system. However, there may be duplicate files present in the other channels. For example, issue the following command:

```
rhncfg-manager list config-channel-14
```

and observe the following output:

```
 Files in config channel 'config-channel-14' /etc/example-config.txt
/etc/rhn/rhn.conf
```

You may then wonder where the second version of **/etc/example-config.txt** went. The rank of the **/etc/example-config.txt** file in **config-channel-17** was higher than that of the same file in **config-channel-14**. As a result, the version of the configuration file in **config-channel-14** is not deployed for this system, although the file still resides in the channel. The **rhncfg-client** command does not list the file because it will not be deployed on this system.

A.2.2. Getting a Config File

To download the most relevant configuration file for the machine, issue the command:

```
rhncfg-client get /etc/example-config.txt
```

You should see output resembling:

```
Deploying /etc/example-config.txt
```

You may then view the contents of the file with **less** or another pager. Note that the file is selected as the most relevant based upon the rank of the config channel containing it. This is accomplished within the **Configuration** tab of the **System Details** page. Refer to Section 6.4.2.9, “System Details” for instructions.

A.2.3. Viewing Config Channels

To view the labels and names of the config channels that apply to the system, issue the command:

```
rhncfg-client channels
```

You should see output resembling:

```
 Config channels: Label Name ----- ---- config-channel-17 config chan 2
config-channel-14 config chan 1
```

The following table lists the options available for **rhncfg-client get**:

Table A.2. rhncfg-client get options

Option	Description
--topdir=TOPDIR	Make all file operations relative to this string.
-h, --help	Show help message and exit

A.2.4. Differentiating between Config Files

To view the differences between the config files deployed on the system and those stored by RHN, issue the command:

```
rhncfg-client diff
```

The output resembles the following:

```
 --- /tmp/@3603.0.rhn-cfg-tmp 2004-01-13 14:18:31.000000000 -0500 +++
/etc/example-config.txt 2003-12-16 21:35:32.000000000 -0500 @@ -1,3 +1,5 @@
+additional text
```

In addition, you may include the **--topdir** option to compare config files in RHN with those located in an arbitrary (and unused) location on the client system, like so:

```
 [root@ root]# rhncfg-client diff --topdir /home/test/blah/ /usr/bin/diff:
/home/test/blah/etc/example-config.txt: No such file or directory
/usr/bin/diff: /home/test/blah/var/spool/aalib.rpm: No such file or directory
```

A.2.5. Verifying Config Files

To quickly determine if client configuration files are different than those associated with it via RHN, issue the command:

```
rhncfg-client verify
```

The output resembles the following:

```
 modified /etc/example-config.txt /var/spool/aalib.rpm
```

The file **example-config.txt** is locally modified, while **aalib.rpm** is not.

The following table lists the options available for **rhncfg-client verify**:

Table A.3. rhncfg-client verify options

Option	Description
-v, --verbose	Increase the amount of output detail. Displays differences in the mode, owner, and group permissions for the specified config file.
-h, --help	Show help message and exit

A.3. Red Hat Network Configuration Manager

Unlike the **Red Hat Network Configuration Client**, the **Red Hat Network Configuration Manager** (**rhncfg-manager**) is designed to maintain RHN's central repository of config files and channels, not those located on client systems. This tool offers a command line alternative to the configuration management features within the RHN website, as well as the ability to script some or all of the related maintenance.

It is intended for use by Config Administrators and requires an RHN username and password that has the appropriate permission set. The username may be specified in **/etc/sysconfig/rhn/rhncfg-manager.conf** or in the [rhncfg-manager] section of **~/.rhncfgrc**.

When the **Red Hat Network Configuration Manager** is run as root, it attempts to pull in needed configuration values from the **Red Hat Update Agent**. When run as a user other than root, you may

have to make configuration changes within the **~/.rhncfgrc** file. The session file is cached in **~/.rhncfg-manager-session** to prevent logging in for every command.

The default timeout for the **Red Hat Network Configuration Manager** is 30 minutes. To alter this, add the **server.session_lifetime** option and new value to the **/etc/rhn/rhn.conf** file on the server running the manager, like so:

```
server.session_lifetime = 120
```

The **Red Hat Network Configuration Manager** offers these primary modes: add, create-channel, diff, diff-revisions, download-channel, get, list, list-channels, remove, remove-channel, revisions, update, and upload-channel.

Each mode offers its own set of options, which can be seen by issuing the following command:

```
rhncfg-manager mode --help
```

Replace ***mode*** with the name of the mode to be inspected:

```
rhncfg-manager diff-revisions --help
```

You can see such a list of options for the add mode at Table A.4, “**rhncfg-manager add** options”.

A.3.1. Creating a Config Channel

To create a config channel for your organization, issue the command:

```
rhncfg-manager create-channel channel-label
```

If prompted for your RHN username and password, provide them. The output resembles the following:

```
Red Hat Network username: rhn-user Password: Creating config channel channel-
label Config channel channel-label created
```

Once you have created a config channel, use the remaining modes listed above to populate and maintain that channel.

A.3.2. Adding Files to a Config Channel

To add a file to a config channel, specify the channel label as well as the local file to be uploaded, such as:

```
rhncfg-manager add --channel=channel-label /path/to/file
```

In addition to the required channel label and the path to the file, you may use the available options for modifying the file during its addition. For instance, you may alter the path and file name by including the **--dest-file** option in the command, like:

```
rhncfg-manager add --channel=channel-label--dest-
file=/new/path/to/file.txt/path/to/file
```

The output resembles the following:

```
 Pushing to channel example-channel Local file >/path/to/file -> remote file
/new/path/to/file.txt
```

The following table lists the options available for **rhncfg-manager add**:

Table A.4. rhncfg-manager add options

Option	Description
-cCHANNEL --channel=CHANNEL	Upload files in this config channel
-dDEST_FILE --dest-file=DEST_FILE	Upload the file as this path
--delim-start=DELIM_START	Start delimiter for variable interpolation
--delim-end=DELIM_END	End delimiter for variable interpolation
-h, --help	show help message and exit

A.3.3. Differentiating between Latest Config Files

To view the differences between the config files on disk and the latest revisions in a channel, issue the command:

```
 rhncfg-manager diff --channel=channel-label --dest-file=/path/to/file.txt \
/local/path/to/file
```

You should see output resembling:

```
 /tmp/dest_path/example-config.txt /home/test/blah/hello_world.txt ---
/tmp/dest_path/example-config.txt config_channel: example-channel revision: 1
+++ /home/test/blah/hello_world.txt 2003-12-14 19:08:59.000000000 -0500 @@ -1
+1 @@ -foo +hello, world
```

The following table lists the options available for **rhncfg-manager diff**:

Table A.5. rhncfg-manager diff options

Option	Description
-cCHANNEL, --channel=CHANNEL	Get file(s) from this config channel
-rREVISION, --revision=REVISION	Use this revision
-dDEST_FILE, --dest-file=DEST_FILE	Upload the file as this path
-tTOPDIR, --topdir=TOPDIR	Make all files relative to this string
-h, --help	Show help message and exit

A.3.4. Differentiating between Various Versions

To compare different versions of a file across channels and revisions, use the **-r** flag to indicate which revision of the file should be compared and the **-n** flag to identify the two channels to be checked. Refer to Section A.3.11, “Determining the Number of File Revisions” for related instructions. Specify only one file name here, since you are comparing the file against another version of itself. For example:

```
 rhncfg-manager diff-revisions -n=channel-label1-r=1-n=channel-label2-
r=1/path/to/file.txt
```

The output resembles the following:

```
 --- /tmp/dest_path/example-config.txt 2004-01-13 14:36:41 \ config channel:
example-channel2 revision: 1 --- /tmp/dest_path/example-config.txt 2004-01-13
14:42:42 \ config channel: example-channel3 revision: 1 @@ -1 +1,20 @@ -foo
+blaaaaaaaaaaaaaaah +-----BEGIN PGP SIGNATURE----- +Version: GnuPG v1.0.6
(GNU/Linux) +Comment: For info see http://www.gnupg.org +
+iD8DBQA9ZY6vse4XmfJPGwgRAsHcAJ9ud9dabUcdscdcqB8AZP7e0Fua0NmKsdhQCeOWHX
+VsDTfen2NWdwwPaTM+S+Cow= +=Ltp2 +-----END PGP SIGNATURE-----
```

The following table lists the options available for **rhncfg-manager diff-revisions**:

Table A.6. rhncfg-manager diff-revisions options

Option	Description
-cCHANNEL, --channel=CHANNEL	Use this config channel
-rREVISION, --revision=REVISION	Use this revision
-h, --help	Show help message and exit

A.3.5. Downloading All Files in a Channel

To download all the files in a channel to disk, create a directory and issue the following command:

```
  rhncfg-manager download-channel channel-label --topdir .
```

The output resembles the following:

```
 Copying /tmp/dest_path/example-config.txt -> \ blah2/tmp/dest_path/example-
config.txt
```

The following table lists the options available for **rhncfg-manager download-channel**:

Table A.7. rhncfg-manager download-channel options

Option	Description
-tTOPDIR, --topdir=TOPDIR	Directory all the file paths are relative to. This option must be set.
-h, --help	Show help message and exit

A.3.6. Getting the Contents of a File

To direct the contents of a particular file to stdout, issue the command:

```
  rhncfg-manager get --channel=channel-label \ /tmp/dest_path/example-config.txt
```

You should see the contents of the file as output.

A.3.7. Listing All Files in a Channel

To list all the files in a channel, issue the command:

```
rhncfg-manager list channel-label
```

You should see output resembling:

```
Files in config channel `example-channel3': /tmp/dest_path/example-config.txt
```

The following table lists the options available for **rhncfg-manager get**:

Table A.8. rhncfg-manager get options

Option	Description
-cCHANNEL, --channel=CHANNEL	Get file(s) from this config channel
-tTOPDIR, --topdir=TOPDIR	Make all files relative to this string
-rREVISION, --revision=REVISION	Get this file revision
-h, --help	Show help message and exit

A.3.8. Listing All Config Channels

To list all of your organization's configuration channels, issue the command:

```
rhncfg-manager list-channels
```

The output resembles the following:

```
Available config channels: example-channel example-channel2 example-channel3
config-channel-14 config-channel-17
```

Note that this does not list **local_override** or **server_import** channels.

A.3.9. Removing a File from a Channel

To remove a file from a channel, issue the command:

```
rhncfg-manager remove --channel=channel-label /tmp/dest_path/example-
config.txt
```

If prompted for your RHN username and password, provide them. You should see output resembling:

```
Red Hat Network username: rhn-user Password: Removing from config channel
example-channel3 /tmp/dest_path/example-config.txt removed
```

The following table lists the options available for **rhncfg-manager remove**:

Table A.9. `rhncfg-manager remove` options

Option	Description
-cCHANNEL, --channel=CHANNEL	Remove files from this config channel
-tTOPDIR, --topdir=TOPDIR	Make all files relative to this string
-h, --help	Show help message and exit

A.3.10. Deleting a Config Channel

To destroy a config channel in your organization, issue the command:

```
rhncfg-manager remove-channel channel-label
```

The output resembles the following:

```
 Removing config channel example-channel Config channel example-channel
removed
```

A.3.11. Determining the Number of File Revisions

To find out how many revisions (revisions go from 1 to N where N is an integer greater than 0) of a file/path are in a channel, issue the following command:

```
 rhncfg-manager revisions channel-label /tmp/dest_path/example-config.txt
```

The output resembles the following:

```
 Analyzing files in config channel example-channel \ /tmp/dest_path/example-
config.txt: 1
```

A.3.12. Updating a File in a Channel

To create a new revision of a file in a channel (or add the first revision to that channel if none existed before for the given path), issue the following command:

```
 rhncfg-manager update \ --channel=channel-label --dest-file=/path/to/file.txt
/local/path/to/file
```

The output resembles the following:

```
 Pushing to channel example-channel: Local file example-
channel/tmp/dest_path/example-config.txt -> \ remote file
/tmp/dest_path/example-config.txt
```

The following table lists the options available for **`rhncfg-manager update`**:

Table A.10. `rhncfg-manager update` options

Option	Description
-cCHANNEL, --channel=CHANNEL	Upload files in this config channel
-dDEST_FILE, --dest-file=DEST_FILE	Upload the file as this path
-tTOPDIR, --topdir=TOPDIR	Make all files relative to this string
--delim-start=DELIM_START	Start delimiter for variable interpolation
--delim-end=DELIM_END	End delimiter for variable interpolation
-h, --help	Show help message and exit

A.3.13. Uploading Multiple Files at Once

To upload multiple files to a config channel from local disk at once, issue the command:

```
rhncfg-manager upload-channel --topdir=topdir channel-label
```

The output resembles the following:

```
Using config channel example-channel4 Uploading /tmp/ola_world.txt from
blah4/tmp/ola_world.txt
```

The following table lists the options available for **`rhncfg-manager upload-channel`**:

Table A.11. `rhncfg-manager upload-channel` options

Option	Description
-tTOPDIR, --topdir=TOPDIR	Directory all the file paths are relative to
-cCHANNEL, --channel=CHANNEL	List of channels the config info will be uploaded into. Channels delimited by ','. Example: --channel=foo,bar,baz
-h, --help	Show help message and exit

RHN API Access

In an effort to provide customers with added flexibility, RHN makes an application programming interface (API) available. This interface can be found by clicking **Help** at the top-right corner of the RHN website, then clicking **API** in the left navigation bar. Or you may go directly to: https://rhn.redhat.com/rpc/api/. Use this URL for your XMLRPC server and your browser.

The RHN API is based upon XML-RPC, which allows distinct pieces of software on disparate systems to make remote procedure calls using XML over HTTP. For this reason, any calls you make are expected to meet the constraints of XML-RPC. You can find out more at http://www.xmlrpc.com/.

This section bypasses a list of available methods and classes in favor of tips for using the API efficiently. These include steps for determining required values and a sample script that makes some of the calls.

B.1. Using the auth Class and Getting the Session

It is worth noting that you will almost invariably use the auth class first. This class offers a single method, login. Use this to establish an RHN session. It requires values for three parameters: username, password, and duration. The first two come directly from your RHN account, while the third is the length of time the session should last in seconds, typically 1200. It returns a session string than can be used in all other methods.

B.2. Obtaining the system_id

Many of the methods require a value for the **system_id** parameter. This is the unique alphanumeric value assigned to each system when registered to RHN. It can be found within the **/etc/sysconfig/rhn/systemid** file on each machine. In addition, you may use the **download_system_id** method within the system class to obtain the value.

B.3. Determining the sid

Several methods require a value for the **sid**, or server ID, parameter. Note that this is different from the **system_id**. You may determine the **sid** of a machine in two different ways. First, you can log into the RHN website, click the name of a system, and view the **sid** at the end of the URL in the location bar. It follows the "=" symbol and is part of a string that resembles the following: "index.pxt?sid=1003486534". Second, you may use the **list_user_systems** method within the system class to obtain a list of systems available to the user that contains the associated **sid**s.

B.4. Viewing the cid

Like servers, channels have their own IDs. This value, the **cid**, is a required parameter for some methods, including **set_base_channel** and **set_child_channels**. Also like the **sid**, the **cid** can be obtained through the RHN website. Just click on the name of a channel and view the end of the URL. It follows the "=" symbol, as part of a string that resembles the following: "details.pxt?cid=54".

B.5. Getting the sgid

System groups also have their own IDs. This value, the **sgid**, is a required parameter for the **set_group_membership** method, for instance. Like the **sid** and **cid**, the **sgid** can be obtained

through the RHN website. Just click on the name of a system group and view the end of the URL. It follows the "=" symbol, as part of a string that resembles the following: "details.pxt?sgid=334958". Note that the member parameter within the **`set_group_membership`** method requires only **`yes`** or **`no`** as input to make the association.

B.6. Channel Labels

The architecture of a channel is not always clear from the channel label. Below is a list that shows the correspondence between channel labels and the official title of the architecture they serve.

Table B.1. Channel Labels

Channel Label	Platform
channel-i386-sun-solaris	i386 Solaris
channel-ia32	IA-32
channel-ia64	IA-64
channel-sparc	Sparc
channel-alpha	Alpha
channel-s390	IBM S/390
channel-s390x	IBM System z
channel-iSeries	IBM eServer System i
channel-pSeries	IBM eServer System p
channel-x86_64	AMD64 and Intel EM64T
channel-ppc	PPC
channel-sparc-sun-solaris	Sparc Solaris

This is particularly necessary to know for the channel.software.create method.

B.7. Sample API Script

The following sample script depicts how to construct an RHN API client. Review the comments and links for a full discussion of the calls made.

```
 #!/usr/bin/perl -w use strict; use Frontier::Client; use Data::Dumper;
################################################################################ #
This is a sample script for use of the experimental RHN Management APIs. # #
The API is currently available using XMLRPC only, which is described in # #
depth at: # # # # http://www.xmlrpc.com/ # # # # We use the Frontier modules,
available from: # # # # http://theoryx5.uwinnipeg.ca/mod_perl/cpan-search?
dist=Frontier-RPC # # #
################################################################################
################################################################################ #
Defining an XMLRPC session. #
################################################################################ #
Define the host first. This will be the FQDN of your satellite system. my
$HOST = 'satellite.server.yourdomain.com'; # Now we create the client object
that will be used throughout the session. my $client = new
Frontier::Client(url => "http://$HOST/rpc/api"); # Next, we execute a login
call, which returns a session identifier that will # be passed in all
subsequent calls. The syntax of this call is described at: # #
http://$HOST/rpc/api/auth/login/ my $session = $client->call('auth.login',
'username', 'password');
################################################################################ #
System calls. #
################################################################################ #
This next call returns a list of systems available to the user. The # syntax
of this call is described at: # #
http://$HOST/rpc/api/system/list_user_systems/ # # In the code snippet below,
we dump data about our systems, and we # capture the ID of the first system we
find for future operations. my $systems = $client-
>call('system.list_user_systems', $session); for my $system (@$systems) {
print Dumper($system); } print "\n\nCapturing ID of system @$systems[0]-
>{name}\n\n"; my $systemid = @$systems[0]->{id}; # This next call returns a
list of packages present on this system. The # syntax of this call is
described at: # # http://$HOST/rpc/api/system/list_packages/ # # This will
probably be a pretty long list. my $packages = $client-
>call('system.list_packages', $session, $systemid); for my $package
(@$packages) { print Dumper($package); } # Additional system calls are
described at: # http://$HOST/rpc/api/system/
```

Probes

As described in Section 6.9, “Monitoring — ”, Monitoring-entitled systems can have probes applied to them that constantly confirm their health and full operability. This appendix lists the available probes broken down by command group, such as Apache.

Many probes that monitor internal system aspects (such as the Linux::Disk Usage probe) rather than external aspects (such as the Network Services::SSH probe) require the installation of the Red Hat Network Monitoring Daemon (**rhnmd**). This requirement is noted within the individual probe reference.

Each probe has its own reference in this appendix that identifies required fields (marked with *), default values, and the thresholds that may be set to trigger alerts. Similarly, the beginning of each command group's section contains information applicable to all probes in that group. Section C.1, “Probe Guidelines” covers general guidelines; the remaining sections examine individual probes.

Note

Nearly all of the probes use *Transmission Control Protocol* (TCP) as their transport protocol. Exceptions to this are noted within the individual probe references.

C.1. Probe Guidelines

The following general guidelines outline the meaning of each probe state, and provide guidance in setting thresholds for your probes.

The following list provides a brief description of the meaning of each probe state:

Unknown

The probes that cannot collect the metrics needed to determine probe state. Most (though not all) probes enter this state when exceeding their timeout period. Probes in this state may be configured incorrectly, as well.

Pending

The probes whose data has not been received by the RHN Satellite. It is normal for new probes to be in this state. However, if all probes move into this state, your monitoring infrastructure may be failing.

OK

The probes that have run successfully without error. This is the desired state for all probes.

Warning

The probes that have crossed their WARNING thresholds.

Critical

The probes that have crossed their CRITICAL thresholds or reached a critical status by some other means. (Some probes become critical when exceeding their timeout period.)

While adding probes, select meaningful thresholds that, when crossed, notify you and your administrators of problems within your infrastructure. Timeout periods are entered in seconds unless otherwise indicated. Exceptions to these rules are noted within the individual probe references.

Important

Some probes have thresholds based on time. In order for such CRITICAL and WARNING thresholds to work as intended, their values cannot exceed the amount of time allotted to the timeout period. Otherwise, an UNKNOWN status is returned in all instances of extended latency, thereby nullifying the thresholds. For this reason, Red Hat strongly recommends ensuring that timeout periods exceed all timed thresholds.

Remember that Red Hat recommends running your probes without notifications for a time to establish baseline performance for each of your systems. Although the default values provided for probes may suit your needs, every organization has a different environment that may require altering thresholds.

C.2. Apache 1.3.x and 2.0.x

The probes in this section may be applied to instances of the Apache Web server. Although the default values presume you will apply these probes using standard HTTP, you may also use them over secure connections by changing the application protocol to **`https`** and the port to **`443`**.

C.2.1. Apache::Processes

The Apache::Processes probe monitors the processes executed on an Apache Web server and collects the following metrics:

- Data Transferred Per Child — Records data transfer information only on individual children. A child process is one that is created from the parent process or another process.
- Data Transferred Per Slot — The cumulative amount of data transferred by a child process that restarts. The number of slots is configured in the **`httpd.conf`** file using the **`MaxRequestsPerChild`** setting.

The **`ExtendedStatus`** directive in the **`httpd.conf`** file of the Web server must be set to **`On`** for this probe to function properly.

Table C.1. Apache::Processes settings

Field	Value
Application Protocol*	http
Port*	80
Pathname*	/server-status
UserAgent*	NOCpulse-ApacheUptime/1.0
Username	
Password	
Timeout*	15
Critical Maximum Megabytes Transferred Per Child	
Warning Maximum Megabytes Transferred Per Child	
Critical Maximum Megabytes Transferred Per Slot	
Warning Maximum Megabytes Transferred Per Slot	

C.2.2. Apache::Traffic

The Apache::Traffic probe monitors the requests on an Apache Web server and collects the following metrics:

- Current Requests — The number of requests being processed by the server at probe runtime.
- Request Rate — The accesses to the server per second since the probe last ran.
- Traffic — The kilobytes per second of traffic the server has processed since the probe last ran.

The **`ExtendedStatus`** directive in the **`httpd.conf`** file of the Web server must be set to **`On`** for this probe to function properly.

Table C.2. Apache::Traffic settings

Field	Value
Application Protocol*	http
Port*	80
Pathname*	/server-status
UserAgent*	NOCpulse-ApacheUptime/1.0
Username	
Password	
Timeout*	15
Critical Maximum Current Requests (number)	
Warning Maximum Current Requests (number)	
Critical Maximum Request Rate (events per second)	
Warning Maximum Request Rate (events per second)	
Critical Maximum Traffic (kilobytes per second)	
Warning Maximum Traffic (kilobytes per second)	

C.2.3. Apache::Uptime

The Apache::Uptime probe stores the cumulative time since the Web server was last started. No metrics are collected by this probe, which is designed to help track service level agreements (SLAs).

Table C.3. Apache::Uptime settings

Field	Value
Application Protocol*	http
Port*	80
Pathname*	/server-status
UserAgent*	NOCpulse-ApacheUptime/1.0
Username	
Password	
Timeout*	15

C.3. BEA WebLogic 6.x and higher

The probes in this section (with the exception of JDBC Connection Pool) can be configured to monitor the properties of any BEA WebLogic 6.x and higher server (Administration or Managed) running on a given host, even in a clustered environment. Monitoring of a cluster is achieved by sending all SNMP queries to the Administration Server of the domain and then querying its Managed Servers for individual data.

In order to obtain this higher level of granularity, the **`BEA Domain Admin Server`** parameter must be used to differentiate between the Administration Server receiving SNMP queries and the Managed Server undergoing the specified probe. If the host to be probed is the Administration Server, then the **`BEA Domain Admin Server`** parameter can be left blank, and both the SNMP queries and the probe will be sent to it only.

If the host to be probed is a Managed Server, then the IP address of the Administration Server should be provided in the **`BEA Domain Admin Server`** parameter, and the Managed Server name should be included in the **`BEA Server Name`** parameter and appended to the end of the **`SNMP Community String`** field. This causes the SNMP queries to be sent to the Administration Server host, as is required, but redirects the specific probe to the Managed Server host.

It should also be noted that the community string needed for probes run against Managed Server hosts should be in the form of **`community_prefix@managed_server_name`** in order for the SNMP query to return results for the desired Managed Server. Finally, SNMP must be enabled on each monitored system. SNMP support can be enabled and configured through the WebLogic Console.

Please see the documentation that came with your BEA server or information on the BEA website for more details about BEA's community string naming conventions: http://e-docs.bea.com/wls/docs70/snmpman/snmpagent.html

C.3.1. BEA WebLogic::Execute Queue

The BEA WebLogic::Execute Queue probe monitors the WebLogic execute queue and provides the following metrics:

- Idle Execute Threads — The number of execution threads in an idle state.
- Queue Length — The number of requests in the queue.

- Request Rate — The number of requests per second.

This probe's transport protocol is User Datagram Protocol (UDP).

Table C.4. BEA WebLogic::Execute Queue settings

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	myserver
Queue Name*	default
Critical Maximum Idle Execute Threads	
Warning Maximum Idle Execute Threads	
Critical Maximum Queue Length	
Warning Maximum Queue Length	
Critical Maximum Request Rate	
Warning Maximum Request Rate	

C.3.2. BEA WebLogic::Heap Free

The BEA WebLogic::Heap Free probe collects the following metric:

- Heap Free — The percentage of free heap space.

This probe's transport protocol is User Datagram Protocol (UDP).

Table C.5. BEA WebLogic::Heap Free settings

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	myserver
Critical Maximum Heap Free	
Warning Maximum Heap Free	
Warning Minimum Heap Free	
Critical Minimum Heap Free	

C.3.3. BEA WebLogic::JDBC Connection Pool

The BEA WebLogic::JDBC Connection Pool probe monitors the Java Database Connection (JDBC) pool on a domain Admin Server only (no Managed Servers) and collects the following metrics:

- Connections — The number of connections to the JDBC.

- Connections Rate — The speed at which connections are made to the JDBC, measured in connections per second.
- Waiters — The number of sessions waiting to connect to the JDBC.

This probe's transport protocol is User Datagram Protocol (UDP).

Table C.6. BEA WebLogic::JDBC Connection Pool settings

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	myserver
JDBC Pool Name*	MyJDBC Connection Pool
Critical Maximum Connections	
Warning Maximum Connections	
Critical Maximum Connection Rate	
Warning Maximum Connection Rate	
Critical Maximum Waiters	
Warning Maximum Waiters	

C.3.4. BEA WebLogic::Server State

The BEA WebLogic::Server State probe monitors the current state of a BEA Weblogic Web server. If the probe is unable to make a connection to the server, a CRITICAL status results.

This probe's transport protocol is User Datagram Protocol (UDP).

Table C.7. BEA WebLogic::Server State settings

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	

C.3.5. BEA WebLogic::Servlet

The BEA WebLogic::Servlet probe monitors the performance of a particular servlet deployed on a WebLogic server and collects the following metrics:

- High Execution Time — The highest amount of time in milliseconds that the servlet takes to execute since the system was started.
- Low Execution Time — The lowest amount of time in milliseconds that the servlet takes to execute since the system was started.

- Execution Time Moving Average — A moving average of the execution time.
- Execution Time Average — A standard average of the execution time.
- Reload Rate — The number of times the specified servlet is reloaded per minute.
- Invocation Rate — The number of times the specified servlet is invoked per minute.

This probe's transport protocol is User Datagram Protocol (UDP).

Table C.8. BEA WebLogic::Servlet settings

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	1
BEA Domain Admin Server	
BEA Server Name*	myserver
Servlet Name*	
Critical Maximum High Execution Time	
Warning Maximum High Execution Time	
Critical Maximum Execution Time Moving Average	
Warning Maximum Execution Time Moving Average	

C.4. General

The probes in this section are designed to monitor basic aspects of your systems. When applying them, ensure their timed thresholds do not exceed the amount of time allotted to the timeout period. Otherwise, the probe returns an UNKOWN status in all instances of extended latency, thereby nullifying the thresholds.

C.4.1. General::Remote Program

The General::Remote Program probe allows you to run any command or script on your system and obtain a status string. Note that the resulting message will be limited to 1024 bytes.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to execute this probe.

Table C.9. General::Remote Program settings

Field	Value
Command*	
OK Exit Status*	0
Warning Exit Status*	1
Critical Exit Status*	2
Timeout	15

C.4.2. General::Remote Program with Data

The General::Remote Program with Data probe allows you to run any command or script on your system and obtain a value, as well as a status string. To use this probe, you must include XML code in the body of your script. This probe supports the following XML tags:

- <perldata> </perldata>
- <hash> </hash>
- <item key =" "> </item>

The remote program will need to output some iteration of the following code to **STDOUT**:

```
  <perldata> <hash> <item key="data">10</item> <item
key="status_message">status message here</item> </hash> </perldata>
```

The required value for **data** is the data point to be inserted in the database for time-series trending. The **status_message** is optional and can be whatever text string is desired with a maximum length of 1024 bytes. Remote programs that do not include a **status_message** still report the value and status returned.

Requirements — The Red Hat Network Monitoring Daemon (**rhnmd**) must be running on the monitored system to execute this probe. XML is case-sensitive. The **data** item key name cannot be changed and it must collect a number as its value.

Table C.10. General::Remote Program with Data settings

Field	Value
Command*	
OK Exit Status*	0
Warning Exit Status*	1
Critical Exit Status*	2
Timeout	15

C.4.3. General::SNMP Check

The General::SNMP Check probe tests your SNMP server by specifying a single object identifier (OID) in dotted notation (such as **1.3.6.1.2.1.1.1.0**) and a threshold associated with the return value. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the SNMP server to answer a connection request.

Requirements — SNMP must be running on the monitored system to perform this probe. Only integers can be used for the threshold values.

This probe's transport protocol is User Datagram Protocol (UDP).

Table C.11. General::SNMP Check settings

Field	Value
SNMP OID*	
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	2
Timeout*	15
Critical Maximum Value	
Warning Maximum Value	
Warning Minimum Value	
Critical Minimum Value	

C.4.4. General::TCP Check

The General::TCP Check probe tests your TCP server by verifying that it can connect to a system via the specified port number. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the TCP server to answer a connection request.

The probe passes the string specified in the **Send** field upon making a connection. The probe anticipates a response from the system, which should include the substring specified in the **Expect** field. If the expected string is not found, the probe returns a CRITICAL status.

Table C.12. General::TCP Check settings

Field	Value
Send	
Expect	
Port*	1
Timeout*	10
Critical Maximum Latency	
Warning Maximum Latency	

C.4.5. General::UDP Check

The General::UDP Check probe tests your UDP server by verifying that it can connect to a system via the specified port number. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the UDP server to answer a connection request.

The probe passes the string specified in the **Send** field upon making a connection. The probe anticipates a response from the system, which should include the substring specified in the **Expect** field. If the expected string is not found, the probe returns a CRITICAL status.

This probe's transport protocol is User Datagram Protocol (UDP).

Table C.13. General::UDP Check settings

Field	Value
Port*	1
Send	
Expect	
Timeout*	10
Critical Maximum Latency	
Warning Maximum Latency	

C.4.6. General::Uptime (SNMP)

The General::Uptime (SNMP) probe records the time since the device was last started. It uses the SNMP object identifier (OID) to obtain this value. The only error status it will return is UNKNOWN.

Requirements — SNMP must be running on the monitored system and access to the OID must be enabled to perform this probe.

This probe's transport protocol is User Datagram Protocol (UDP).

Table C.14. General::Uptime (SNMP) settings

Field	Value
SNMP Community String*	public
SNMP Port*	161
SNMP Version*	2
Timeout*	15

C.5. Linux

The probes in this section monitor essential aspects of your Linux systems, from CPU usage to virtual memory. Apply them to mission-critical systems to obtain warnings prior to failure.

Unlike other probe groups, which may or may not require the Red Hat Network Monitoring Daemon, every Linux probe requires that the **`rhnmd`** daemon be running on the monitored system.

C.5.1. Linux::CPU Usage

The Linux::CPU Usage probe monitors the CPU utilization on a system and collects the following metric:

- CPU Percent Used — The five-second average of the percent of CPU usage at probe execution.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to run this probe.

Table C.15. Linux::CPU Usage settings

Field	Value
Timeout*	15
Critical Maximum CPU Percent Used	
Warning Maximum CPU Percent Used	

C.5.2. Linux::Disk IO Throughput

The Linux::Disk IO Throughput probe monitors a given disk and collects the following metric:

- Read Rate — The amount of data that is read in kilobytes per second.
- Write Rate — The amount of data that is written in kilobytes per second.

To obtain the value for the required **`Disk number or disk name`** field, run **`iostat`** on the system to be monitored and see what name has been assigned to the disk you desire. The default value of **`0`** usually provides statistics from the first hard drive connected directly to the system.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to execute this probe. Also, the **`Disk number or disk name`** parameter must match the format visible when the **`iostat`** command is run. If the format is not identical, the configured probe enters an UNKNOWN state.

Table C.16. Linux::Disk IO Throughput settings

Field	Value
Disk number or disk name*	0
Timeout*	15
Critical Maximum KB read/second	
Warning Maximum KB read/second	
Warning Minimum KB read/second	
Critical Minimum KB read/second	
Critical Maximum KB written/second	
Warning Maximum KB written/second	
Warning Minimum KB written/second	
Critical Minimum KB written/second	

C.5.3. Linux::Disk Usage

The Linux::Disk Usage probe monitors the disk space on a specific file system and collects the following metrics:

- File System Used — The percentage of the file system currently in use.
- Space Used — The amount of the file system in megabytes currently in use.
- Space Available — The amount of the file system in megabytes currently available.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to execute this probe.

Table C.17. Linux::Disk Usage settings

Field	Value
File system*	/dev/hda1
Timeout*	15
Critical Maximum File System Percent Used	
Warning Maximum File System Percent Used	
Critical Maximum Space Used	
Warning Maximum Space Used	
Warning Minimum Space Available	
Critical Minimum Space Available	

C.5.4. Linux::Inodes

The Linux::Inodes probe monitors the specified file system and collects the following metric:

- Inodes — The percentage of inodes currently in use.

An inode is a data structure that holds information about files in a Linux file system. There is an inode for each file, and a file is uniquely identified by the file system on which it resides and its inode number on that system.

Requirements — The Red Hat Network Monitoring Daemon (**rhnmd**) must be running on the monitored system to execute this probe.

Table C.18. Linux::Inodes settings

Field	Value
File system*	/
Timeout*	15
Critical Maximum Inodes Percent Used	
Warning Maximum Inodes Percent Used	

C.5.5. Linux::Interface Traffic

The Linux::Interface Traffic probe measures the amount of traffic into and out of the specified interface (such as eth0) and collects the following metrics:

- Input Rate — The traffic in bytes per second going into the specified interface.
- Output Rate — The traffic in bytes per second going out of the specified interface.

Requirements — The Red Hat Network Monitoring Daemon (**rhnmd**) must be running on the monitored system to execute this probe.

Table C.19. Linux::Interface Traffic settings

Field	Value
Interface*	
Timeout*	30
Critical Maximum Input Rate	
Warning Maximum Input Rate	
Warning Minimum Input Rate	
Critical Minimum Input Rate	
Critical Maximum Output Rate	
Warning Maximum Output Rate	
Warning Minimum Output Rate	
Critical Minimum Output Rate	

C.5.6. Linux::Load

The Linux::Load probe monitors the CPU of a system and collects the following metric:

- Load — The average load on the system CPU over various periods.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to execute this probe.

Table C.20. Linux::Load settings

Field	Value
Timeout*	15
Critical CPU Load 1-minute average	
Warning CPU Load 1-minute average	
Critical CPU Load 5-minute average	
Warning CPU Load 5-minute average	
Critical CPU Load 15-minute average	
Warning CPU Load 15-minute average	

C.5.7. Linux::Memory Usage

The Linux::Memory Usage probe monitors the memory on a system and collects the following metric:

- RAM Free — The amount of free random access memory (RAM) in megabytes on a system.

You can also include the reclaimable memory in this metric by entering **`yes`** or **`no`** in the **`Include reclaimable memory`** field.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to execute this probe.

Table C.21. Linux::Memory Usage settings

Field	Value
Include reclaimable memory	no
Timeout*	15
Warning Maximum RAM Free	
Critical Maximum RAM Free	

C.5.8. Linux::Process Counts by State

The Linux::Process Counts by State probe identifies the number of processes in the following states:

- Blocked — A process that has been switched to the waiting queue and whose state has been switched to **`waiting`**.
- Defunct — A process that has terminated (either because it has been killed by a signal or because it has called **`exit()`**) and whose parent process has not yet received notification of its termination by executing some form of the **`wait()`** system call.
- Stopped — A process that has been stopped before its execution could be completed.
- Sleeping — A process that is in the **`Interruptible`** sleep state and that can later be reintroduced into memory, resuming execution where it left off.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to execute this probe.

Table C.22. Linux::Process Counts by State settings

Field	Value
Timeout*	15
Critical Maximum Blocked Processes	
Warning Maximum Blocked Processes	
Critical Maximum Defunct Processes	
Warning Maximum Defunct Processes	
Critical Maximum Stopped Processes	
Warning Maximum Stopped Processes	
Critical Maximum Sleeping Processes	
Warning Maximum Sleeping Processes	
Critical Maximum Child Processes	
Warning Maximum Child Processes	

C.5.9. Linux::Process Count Total

The Linux::Process Count Total probe monitors a system and collects the following metric:

- Process Count — The total number of processes currently running on the system.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to execute this probe.

Table C.23. Linux::Process Count Total settings

Field	Value
Timeout*	15
Critical Maximum Process Count	
Warning Maximum Process Count	

C.5.10. Linux::Process Health

The Linux::Process Health probe monitors user-specified processes and collects the following metrics:

- CPU Usage — The CPU usage rate for a given process in milliseconds per second. This metric reports the **`time`** column of **`ps`** output, which is the cumulative CPU time used by the process. This makes the metric independent of probe interval, allows sane thresholds to be set, and generates usable graphs (i.e. a sudden spike in CPU usage shows up as a spike in the graph).
- Child Process Groups — The number of child processes spawned from the specified parent process. A child process inherits most of its attributes, such as open files, from its parent.
- Threads — The number of running threads for a given process. A thread is the basic unit of CPU utilization, and consists of a program counter, a register set, and a stack space. A thread is also called a lightweight process.
- Physical Memory Used — The amount of physical memory (or RAM) in kilobytes used by the specified process.
- Virtual Memory Used — The amount of virtual memory in kilobytes used by the specified process, or the size of the process in real memory plus swap.

Specify the process by its command name or process ID. (PID). Entering a PID overrides the entry of a command name. If no command name or PID is entered, the error **`Command not found`** is displayed and the probe will be set to a CRITICAL state.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to execute this probe.

Table C.24. Linux::Process Health settings

Field	Value
Command Name	
Process ID (PID) file	
Timeout*	15
Critical Maximum CPU Usage	
Warning Maximum CPU Usage	
Critical Maximum Child Process Groups	
Warning Maximum Child Process Groups	
Critical Maximum Threads	
Warning Maximum Threads	
Critical Maximum Physical Memory Used	
Warning Maximum Physical Memory Used	
Critical Maximum Virtual Memory Used	
Warning Maximum Virtual Memory Used	

C.5.11. Linux::Process Running

The Linux::Process Running probe verifies that the specified process is functioning properly. It counts either processes or process groups, depending on whether the **`Count process groups`** checkbox is selected.

By default, the checkbox is selected, thereby indicating that the probe should count the number of process group leaders independent of the number of children. This allows you, for example, to verify that two instances of the Apache Web server are running regardless of the (dynamic) number of child processes. If it is not selected, the probe conducts a straightforward count of the number of processes (children and leaders) matching the specified process.

Specify the process by its command name or process ID. (PID). Entering a PID overrides the entry of a command name. If no command name or PID is entered, the error **`Command not found`** is displayed and the probe enters a CRITICAL state.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to execute this probe.

Table C.25. Linux::Process Running settings

Field	Value
Command name	
PID file	
Count process groups	(checked)
Timeout*	15
Critical Maximum Number Running	
Critical Minimum Number Running	

C.5.12. Linux::Swap Usage

The Linux::Swap Usage probe monitors the swap partitions running on a system and reports the following metric:

- Swap Free — The percent of swap memory currently free.

Requirements — The Red Hat Network Monitoring Daemon (**rhnmd**) must be running on the monitored system to execute this probe.

Table C.26. Linux::Swap Usage settings

Field	Value
Timeout*	15
Warning Minimum Swap Free	
Critical Minimum Swap Free	

C.5.13. Linux::TCP Connections by State

The Linux::TCP Connections by State probe identifies the total number of TCP connections, as well as the quantity of each in the following states:

- TIME_WAIT — The socket is waiting after close for remote shutdown transmission so it may handle packets still in the network.
- CLOSE_WAIT — The remote side has been shut down and is now waiting for the socket to close.
- FIN_WAIT — The socket is closed, and the connection is now shutting down.
- ESTABLISHED — The socket has a connection established.
- SYN_RCVD — The connection request has been received from the network.

This probe can be helpful in finding and isolating network traffic to specific IP addresses or examining network connections into the monitored system.

The filter parameters for the probe let you narrow the probe's scope. This probe uses the **netstat -ant** command to retrieve data. The **Local IP address** and **Local port** parameters use values in the **Local Address** column of the output; the **Remote IP address** and **Remote port** parameters use values in the **Foreign Address** column of the output for reporting.

Requirements — The Red Hat Network Monitoring Daemon (**rhnmd**) must be running on the monitored system to execute this probe.

Table C.27. Linux::TCP Connections by State settings

Field	Value
Local IP address filter pattern list	
Local port number filter	
Remote IP address filter pattern list	
Remote port number filter	
Timeout*	15
Critical Maximum Total Connections	
Warning Maximum Total Connections	
Critical Maximum TIME_WAIT Connections	
Warning Maximum TIME_WAIT Connections	
Critical Maximum CLOSE_WAIT Connections	
Warning Maximum CLOSE_WAIT Connections	
Critical Maximum FIN_WAIT Connections	
Warning Maximum FIN_WAIT Connections	
Critical Maximum ESTABLISHED Connections	
Warning Maximum ESTABLISHED Connections	
Critical Maximum SYN_RCVD Connections	
Warning Maximum SYN_RCVD Connections	

C.5.14. Linux::Users

The Linux::Users probe monitors the users of a system and reports the following metric:

- Users — The number of users currently logged in.

Requirements — The Red Hat Network Monitoring Daemon (**rhnmd**) must be running on the monitored system to execute this probe.

Table C.28. Linux::Users settings

Field	Value
Timeout*	15
Critical Maximum Users	
Warning Maximum Users	

C.5.15. Linux::Virtual Memory

The Linux::Virtual Memory probe monitors the total system memory and collects the following metric:

- Virtual Memory — The percent of total system memory - random access memory (RAM) plus swap - that is free.

Requirements — The Red Hat Network Monitoring Daemon (**rhnmd**) must be running on the monitored system to execute this probe.

Table C.29. Linux::Virtual Memory settings

Field	Value
Timeout*	15
Warning Minimum Virtual Memory Free	
Critical Minimum Virtual Memory Free	

C.6. LogAgent

The probes in this section monitor the log files on your systems. You can use them to query logs for certain expressions and track the sizes of files. For LogAgent probes to run, the **nocpulse** user must be granted read access to your log files.

Note that data from the first run of these probes is not measured against the thresholds to prevent spurious notifications caused by incomplete metric data. Measurements will begin on the second run.

C.6.1. LogAgent::Log Pattern Match

The LogAgent::Log Pattern Match probe uses regular expressions to match text located within the monitored log file and collects the following metrics:

- Regular Expression Matches — The number of matches that have occurred since the probe last ran.
- Regular Expression Match Rate — The number of matches per minute since the probe last ran.

Requirements — The Red Hat Network Monitoring Daemon (**rhnmd**) must be running on the monitored system to execute this probe. For this probe to run, the **nocpulse** user must be granted read access to your log files.

In addition to the name and location of the log file to be monitored, you must provide a regular expression to be matched against. The expression must be formatted for **egrep**, which is equivalent to **grep -E** and supports extended regular expressions. This is the regular expression set for **egrep**:

```
 ^ beginning of line $ end of line . match one char * match zero or more chars
[] match one character set, e.g. '[Ff]oo' [^] match not in set '[^A-F]oo' +
match one or more of preceding chars ? match zero or one of preceding chars |
or, e.g. a|b () groups chars, e.g., (foo|bar) or (foo)+
```

Warning

Do not include single quotation marks (') within the expression. Doing so causes **egrep** to fail silently and the probe to time out.

Table C.30. LogAgent::Log Pattern Match settings

Field	Value
Log file*	/var/log/messages
Basic regular expression*	
Timeout*	45
Critical Maximum Matches	
Warning Maximum Matches	
Warning Minimum Matches	
Critical Minimum Matches	
Critical Maximum Match Rate	
Warning Maximum Match Rate	
Warning Minimum Match Rate	
Critical Maximum Match Rate	

C.6.2. LogAgent::Log Size

The LogAgent::Log Size probe monitors log file growth and collects the following metrics:

- Size — The size the log file has grown in bytes since the probe last ran.
- Output Rate — The number of bytes per minute the log file has grown since the probe last ran.
- Lines — The number of lines written to the log file since the probe last ran.
- Line Rate — The number of lines written per minute to the log file since the probe last ran.

Requirements — The Red Hat Network Monitoring Daemon (**`rhnmd`**) must be running on the monitored system to execute this probe. For this probe to run, the **`nocpulse`** user must be granted read access to your log files.

Table C.31. LogAgent::Log Size settings

Field	Value
Log file*	/var/log/messages
Timeout*	20
Critical Maximum Size	
Warning Maximum Size	
Warning Minimum Size	
Critical Minimum Size	
Critical Maximum Output Rate	
Warning Maximum Output Rate	
Warning Minimum Output Rate	
Critical Minimum Output Rate	
Critical Maximum Lines	
Warning Maximum Lines	
Warning Minimum Lines	
Critical Minimum Lines	
Critical Maximum Line Rate	
Warning Maximum Line Rate	
Warning Minimum Line Rate	
Critical Minimum Line Rate	

C.7. MySQL 3.23 - 3.33

The probes in this section monitor aspects of the MySQL database using the **`mysqladmin`** binary. No specific user privileges are needed for these probes.

Note that the **`mysql-server`** package must be installed on the system conducting the monitoring for these probes to complete. Refer to the MySQL Installation section of the *RHN Satellite Installation Guide* for instructions.

C.7.1. MySQL::Database Accessibility

The MySQL::Database Accessibility probe tests connectivity through a database account that has no database privileges. If no connection is made, a CRITICAL status results.

Table C.32. MySQL::Database Accessibility settings

Field	Value
Username*	
Password	
MySQL Port	3306
Database*	mysql
Timeout	15

C.7.2. MySQL::Opened Tables

The MySQL::Opened Tables probe monitors the MySQL server and collects the following metric:

- Opened Tables — The tables that have been opened since the server was started.

Table C.33. MySQL::Opened Tables settings

Field	Value
Username	
Password	
MySQL Port*	3306
Timeout	15
Critical Maximum Opened Objects	
Warning Maximum Opened Objects	
Warning Minimum Opened Objects	
Critical Minimum Opened Objects	

C.7.3. MySQL::Open Tables

The MySQL::Open Tables probe monitors the MySQL server and collects the following metric:

- Open Tables — The number of tables open when the probe runs.

Table C.34. MySQL::Open Tables settings

Field	Value
Username	
Password	
MySQL Port*	3306
Timeout	15
Critical Maximum Open Objects	
Warning Maximum Open Objects	
Warning Minimum Open Objects	
Critical Minimum Open Objects	

C.7.4. MySQL::Query Rate

The MySQL::Query Rate probe monitors the MySQL server and collects the following metric:

- Query Rate — The average number of queries per second per database server.

Table C.35. MySQL::Query Rate settings

Field	Value
Username	
Password	
MySQL Port*	3306
Timeout	15
Critical Maximum Query Rate	
Warning Maximum Query Rate	
Warning Minimum Query Rate	
Critical Minimum Query Rate	

C.7.5. MySQL::Threads Running

The MySQL::Threads Running probe monitors the MySQL server and collects the following metric:

- Threads Running — The total number of running threads within the database.

Table C.36. MySQL::Threads Running settings

Field	Value
Username	
Password	
MySQL Port*	3306
Timeout	15
Critical Maximum Threads Running	
Warning Maximum Threads Running	
Warning Minimum Threads Running	
Critical Minimum Threads Running	

C.8. Network Services

The probes in this section monitor various services integral to a functioning network. When applying them, ensure that their timed thresholds do not exceed the amount of time allotted to the timeout period. Otherwise, an UNKNOWN status is returned in all instances of extended latency, thereby nullifying the thresholds.

C.8.1. Network Services::DNS Lookup

The Network Services::DNS Lookup probe uses the **`dig`** command to see if it can resolve the system or domain name specified in the **`Host or Address to look up`** field. It collects the following metric:

- Query Time — The time in milliseconds required to execute the **`dig`** request.

This is useful in monitoring the status of your DNS servers. To monitor one of your DNS servers, supply a well-known host/domain name, such as a large search engine or corporate Web site.

Table C.37. Network Services::DNS Lookup settings

Field	Value
Host or Address to look up	
Timeout*	10
Critical Maximum Query Time	
Warning Maximum Query Time	

C.8.2. Network Services::FTP

The Network Services::FTP probe uses network sockets to test FTP port availability. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the FTP server to answer a connection request.

This probe supports authentication. Provide a username and password in the appropriate fields to use this feature.The optional **Expect** value is the string to be matched against after a successful connection is made to the FTP server. If the expected string is not found, the probe returns a CRITICAL state.

Table C.38. Network Services::FTP settings

Field	Value
Expect	FTP
Username	
Password	
FTP Port*	21
Timeout*	10
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

C.8.3. Network Services::IMAP Mail

The Network Services::IMAP Mail probe determines if it can connect to the IMAP 4 service on the system. Specifying an optional port will override the default port 143. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the IMAP server to answer a connection request.

The required **Expect** value is the string to be matched against after a successful connection is made to the IMAP server. If the expected string is not found, the probe returns a CRITICAL state.

Table C.39. Network Services::IMAP Mail settings

Field	Value
IMAP Port*	143
Expect*	OK
Timeout*	5
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

C.8.4. Network Services::Mail Transfer (SMTP)

The Network Services::Mail Transfer (SMTP) probe determines if it can connect to the SMTP port on the system. Specifying an optional port number overrides the default port 25. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the SMTP server to answer a connection request.

Table C.40. Network Services::Mail Transfer (SMTP) settings

Field	Value
SMTP Port*	25
Timeout*	10
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

C.8.5. Network Services::Ping

The Network Services::Ping probe determines if the RHN Server can **`ping`** the monitored system or a specified IP address. It also checks the packet loss and compares the round trip average against the Warning and Critical threshold levels. The required **`Packets to send`** value allows you to control how many ICMP ECHO packets are sent to the system. This probe collects the following metrics:

- Round-Trip Average — The time it takes in milliseconds for the ICMP ECHO packet to travel to and from the monitored system.
- Packet Loss — The percent of data lost in transit.

Although optional, the **`IP Address`** field can be instrumental in collecting metrics for systems that have multiple IP addresses. For instance, if the system is configured with multiple virtual IP addresses or uses Network Address Translation (NAT) to support internal and external IP addresses, this option may be used to check a secondary IP address rather than the primary address associated with the hostname.

Note that this probe conducts the **`ping`** from an RHN Server and not the monitored system. Populating the IP Address field does not test connectivity between the system and the specified IP address but between the RHN Server and the IP address. Therefore, entering the same IP address for Ping probes on different systems accomplishes precisely the same task. To conduct a **`ping`** from a monitored system to an individual IP address, use the Remote Ping probe instead. Refer to Section C.8.7, “Network Services::Remote Ping”.

Table C.41. Network Services::Ping settings

Field	Value
IP Address (defaults to system IP)	
Packets to send*	20
Timeout*	10
Critical Maximum Round-Trip Average	
Warning Maximum Round-Trip Average	
Critical Maximum Packet Loss	
Warning Maximum Packet Loss	

C.8.6. Network Services::POP Mail

The Network Services::POP Mail probe determines if it can connect to the POP3 port on the system. A port number must be specified; specifying another port number overrides the default port 110. This probe collects the following metric:

- Remote Service Latency — The time it takes in seconds for the POP server to answer a connection request.

The required **Expect** value is the string to be matched against after a successful connection is made to the POP server. The probe looks for the string in the first line of the response from the system. The default is **+OK**. If the expected string is not found, the probe returns a CRITICAL state.

Table C.42. Network Services::POP Mail settings

Field	Value
Port*	110
Expect*	+OK
Timeout*	10
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

C.8.7. Network Services::Remote Ping

The Network Services::Remote Ping probe determines if the monitored system can **ping** a specified IP address. It also monitors the packet loss and compares the round trip average against the Warning and Critical threshold levels. The required **Packets to send** value allows you to control how many ICMP ECHO packets are sent to the address. This probe collects the following metrics:

- Round-Trip Average — The time it takes in milliseconds for the ICMP ECHO packet to travel to and from the IP address.
- Packet Loss — The percent of data lost in transit.

The **IP Address** field identifies the precise address to be pinged. Unlike the similar, optional field in the standard Ping probe, this field is required. The monitored system directs the ping to a third address, rather than to the RHN Server. Since the Remote Ping probe tests connectivity from the monitored system, another IP address must be specified. To conduct pings from the RHN Server to a system or IP address, use the standard Ping probe instead. Refer to Section C.8.5, “Network Services::Ping”.

Requirements — The Red Hat Network Monitoring Daemon (**rhnmd**) must be running on the monitored system to execute this probe.

Table C.43. Network Services::Remote Ping settings

Field	Value
IP Address*	
Packets to send*	20
Timeout*	10
Critical Maximum Round-Trip Average	
Warning Maximum Round-Trip Average	
Critical Maximum Packet Loss	
Warning Maximum Packet Loss	

C.8.8. Network Services::RPCService

The Network Services::RPCService probe tests the availability of remote procedure call (RPC) programs on a given IP address. It collects the following metric:

- Remote Service Latency — The time it takes in seconds for the RPC server to answer a connection request.

RPC server programs, which provide function calls via that RPC network, register themselves in the RPC network by declaring a program ID and a program name. NFS is an example of a service that works via the RPC mechanism.

Client programs that wish to use the resources of RPC server programs do so by asking the machine on which the server program resides to provide access to RPC functions within the RPC program number or program name. These conversations can occur over either TCP or UDP (but are almost always UDP).

This probe allows you to test simple program availability. You must specify the program name or number, the protocol over which the conversation occurs, and the usual timeout period.

Table C.44. Network Services::RPCService settings

Field	Value
Protocol (TCP/UDP)	udp
Service Name*	nfs
Timeout*	10
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

C.8.9. Network Services::Secure Web Server (HTTPS)

The Network Services::Secure Web Server (HTTPS) probe determines the availability of the secure Web server and collects the following metric:

- Remote Service Latency — The time it takes in seconds for the HTTPS server to answer a connection request.

This probe confirms that it can connect to the HTTPS port on the specified host and retrieve the specified URL. If no URL is specified, the probe fetches the root document. The probe looks for a HTTP/1. message from the system unless you alter that value. Specifying another port number overrides the default port of 443.

This probe supports authentication. Provide a username and password in the appropriate fields to use this feature. Unlike most other probes, this probe returns a CRITICAL status if it cannot contact the system within the timeout period.

Table C.45. Network Services::Secure Web Server (HTTPS) settings

Field	Value
URL Path	/
Expect Header	HTTP/1
Expect Content	
UserAgent*	NOCpulse-check_http/1.0
Username	
Password	
Timeout*	10
HTTPS Port*	443
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

C.8.10. Network Services::SSH

The Network Services::SSH probe determines the availability of SSH on the specified port and collects the following metric:

- Remote Service Latency — The time it takes in seconds for the SSH server to answer a connection request.

Upon successfully contacting the SSH server and receiving a valid response, the probe displays the protocol and server version information. If the probe receives an invalid response, it displays the message returned from the server and generates a WARNING state.

Table C.46. Network Services::SSH settings

Field	Value
SSH Port*	22
Timeout*	5
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

C.8.11. Network Services::Web Server (HTTP)

The Network Services::Web Server (HTTP) probe determines the availability of the Web server and collects the following metric:

- Remote Service Latency — The time it takes in seconds for the HTTP server to answer a connection request.

This probe confirms it can connect to the HTTP port on the specified host and retrieve the specified URL. If no URL is specified, the probe will fetch the root document. The probe looks for a HTTP/1. message from the system, unless you alter that value. Specifying another port number will override the default port of 80. Unlike most other probes, this probe will return a CRITICAL status if it cannot contact the system within the timeout period.

This probe supports authentication. Provide a username and password in the appropriate fields to use this feature. Also, the optional Virtual Host field can be used to monitor a separate documentation set located on the same physical machine presented as a standalone server. If your Web server is not configured to use virtual hosts (which is typically the case), you should leave this field blank. If you do have virtual hosts configured, enter the domain name of the first host here. Add as many probes as necessary to monitor all virtual hosts on the machine.

Table C.47. Network Services::Web Server (HTTP) settings

Field	Value
URL Path	/
Virtual Host	
Expect Header	HTTP/1
Expect Content	
UserAgent*	NOCpulse-check_http/1.0
Username	
Password	
Timeout*	10
HTTP Port*	80
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

C.9. Oracle 8i and 9i

The probes in this section may be applied to instances of the Oracle database matching the versions supported. Oracle probes require the configuration of the database and associations made by running the following command:

```
$ORACLE_HOME/rdbms/admin/catalog.sql
```

In addition, for these probes to function properly, the Oracle user configured in the probe must have minimum privileges of CONNECT and SELECT_CATALOG_ROLE.

Some Oracle probes are specifically aimed at tuning devices for long-term performance gains, rather than avoiding outages. Therefore, Red Hat recommends scheduling them to occur less frequently, between every hour and every two days. This provides a better statistical representation, de-emphasizing anomalies that can occur at shorter time intervals. This applies to following probes: Buffer Cache, Data Dictionary Cache, Disk Sort Ratio, Library Cache, and Redo Log.

For CRITICAL and WARNING thresholds based upon time to work as intended, their values cannot

exceed the amount of time allotted to the timeout period. Otherwise, an UNKNOWN status is returned in all cases of extended latency, thereby nullifying the thresholds. For this reason, Red Hat strongly recommends ensuring that timeout periods exceed all timed thresholds. In this section, this refers specifically to the probe TNS Ping.

Finally, customers using these Oracle probes against a database using Oracle's Multi-Threaded Server (MTS) must contact Red Hat support to have entries added to the RHN Server's /etc/hosts file to ensure that the DNS name is resolved correctly.

C.9.1. Oracle::Active Sessions

The Oracle::Active Sessions probe monitors an Oracle instance and collects the following metrics:

- Active Sessions — The number of active sessions based on the value of **`V$PARAMETER.PROCESSES`**.
- Available Sessions — The percentage of active sessions that are available based on the value of **`V$PARAMETER.PROCESSES`**.

Table C.48. Oracle::Active Sessions settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Critical Maximum Active Sessions	
Warning Maximum Active Sessions	
Critical Maximum Available Sessions Used	
Warning Maximum Available Sessions Used	

C.9.2. Oracle::Availability

The Oracle::Availability probe determines the availability of the database from the RHN Satellite.

Table C.49. Oracle::Availability settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30

C.9.3. Oracle::Blocking Sessions

The Oracle::Blocking Sessions probe monitors an Oracle instance and collects the following metric:

- Blocking Sessions — The number of sessions preventing other sessions from committing changes

to the Oracle database, as determined by the required *Time Blocking* value you provide. Only those sessions that have been blocking for this duration, which is measured in seconds, are counted as blocking sessions.

Table C.50. Oracle::Blocking Sessions settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Time Blocking (seconds)*	20
Timeout*	30
Critical Maximum Blocking Sessions	
Warning Maximum Blocking Sessions	

C.9.4. Oracle::Buffer Cache

The Oracle::Buffer Cache probe computes the Buffer Cache Hit Ratio so as to optimize the system global area (SGA) Database Buffer Cache size. It collects the following metrics:

- Db Block Gets — The number of blocks accessed via single block gets (not through the consistent get mechanism).
- Consistent Gets — The number of accesses made to the block buffer to retrieve data in a consistent mode.
- Physical Reads — The cumulative number of blocks read from disk.
- Buffer Cache Hit Ratio — The rate at which the database goes to the buffer instead of the hard disk to retrieve data. A low ratio suggests more RAM should be added to the system.

Table C.51. Oracle::Buffer Cache settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port	1521
Timeout*	30
Warning Minimum Buffer Cache Hit Ratio	
Critical Minimum Buffer Cache Hit Ratio	

C.9.5. Oracle::Client Connectivity

The Oracle::Client Connectivity probe determines if the database is up and capable of receiving connections from the monitored system. This probe opens an **`rhnmd`** connection to the system and issues a **`sqlplus connect`** command on the monitored system.

The **`Expected DB name`** parameter is the expected value of **`V$DATABASE.NAME`**. This value is case-

insensitive. A CRITICAL status is returned if this value is not found.

Requirements — The Red Hat Network Monitoring Daemon (**rhnmd**) must be running on the monitored system to execute this probe. For this probe to run, the **nocpulse** user must be granted read access to your log files.

Table C.52. Oracle::Client Connectivity settings

Field	Value
Oracle Hostname or IP address*	
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
ORACLE_HOME*	/opt/oracle
Expected DB Name*	
Timeout*	30

C.9.6. Oracle::Data Dictionary Cache

The Oracle::Data Dictionary Cache probe computes the Data Dictionary Cache Hit Ratio so as to optimize the SHARED_POOL_SIZE in **init.ora**. It collects the following metrics:

- Data Dictionary Hit Ratio — The ratio of cache hits to cache lookup attempts in the data dictionary cache. In other words, the rate at which the database goes to the dictionary instead of the hard disk to retrieve data. A low ratio suggests more RAM should be added to the system.
- Gets — The number of blocks accessed via single block gets (not through the consistent get mechanism).
- Cache Misses — The number of accesses made to the block buffer to retrieve data in a consistent mode.

Table C.53. Oracle::Data Dictionary Cache settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Warning Minimum Data Dictionary Hit Ratio	
Critical Minimum Data Dictionary Hit Ratio	

C.9.7. Oracle::Disk Sort Ratio

The Oracle::Disk Sort Ratio probe monitors an Oracle database instance and collects the following metric:

- Disk Sort Ratio — The rate of Oracle sorts that were too large to be completed in memory and were

instead sorted using a temporary segment.

Table C.54. Oracle::Disk Sort Ratio settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Critical Maximum Disk Sort Ratio	
Warning Maximum Disk Sort Ratio	

C.9.8. Oracle::Idle Sessions

The Oracle::Idle Sessions probe monitors an Oracle instance and collects the following metric:

- Idle Sessions — The number of Oracle sessions that are idle, as determined by the required *Time Idle* value you provide. Only those sessions that have been idle for this duration, which is measured in seconds, are counted as idle sessions.

Table C.55. Oracle::Idle Sessions settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Time Idle (seconds)*	20
Timeout*	30
Critical Maximum Idle Sessions	
Warning Maximum Idle Sessions	

C.9.9. Oracle::Index Extents

The Oracle::Index Extents probe monitors an Oracle instance and collects the following metric:

- Allocated Extents — The number of allocated extents for any index.
- Available Extents — The percentage of available extents for any index.

The required **`Index Name`** field contains a default value of `%` that matches any index name.

Table C.56. Oracle::Index Extents settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Index Owner*	%
Index Name*	%
Timeout*	30
Critical Maximum of Allocated Extents	
Warning Maximum of Allocated Extents	
Critical Maximum of Available Extents	
Warning Maximum of Available Extents	

C.9.10. Oracle::Library Cache

The Oracle::Library Cache probe computes the Library Cache Miss Ratio so as to optimize the SHARED_POOL_SIZE in **`init.ora`**. It collects the following metrics:

- Library Cache Miss Ratio — The rate at which a library cache pin miss occurs. This happens when a session executes a statement that it has already parsed but finds that the statement is no longer in the shared pool.
- Executions — The number of times a pin was requested for objects of this namespace.
- Cache Misses — The number of pins of objects with previous pins since the object handle was created that must now retrieve the object from disk.

Table C.57. Oracle::Library Cache settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Critical Maximum Library Cache Miss Ratio	
Warning Maximum Library Cache Miss Ratio	

C.9.11. Oracle::Locks

The Oracle::Locks probe monitors an Oracle database instance and collects the following metric:

- Active Locks — The current number of active locks as determined by the value in the v$locks table. Database administrators should be aware of high numbers of locks present in a database instance.

Locks are used so that multiple users or processes updating the same data in the database do not conflict. This probe is useful for alerting database administrators when a high number of locks are

present in a given instance.

Table C.58. Oracle::Locks settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Critical Maximum Active Locks	
Warning Maximum Active Locks	

C.9.12. Oracle::Redo Log

The Oracle::Redo Log probe monitors an Oracle database instance and collects the following metrics:

- Redo Log Space Request Rate — The average number of redo log space requests per minute since the server has been started.
- Redo Buffer Allocation Retry Rate — The average number of buffer allocation retries per minute since the server was started.

The metrics returned and the thresholds they are measured against are numbers representing the rate of change in events per minute. The rate of change for these metrics should be monitored because fast growth can indicate problems requiring investigation.

Table C.59. Oracle::Redo Log settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Timeout*	30
Critical Maximum Redo Log Space Request Rate	
Warning Maximum Redo Log Space Request Rate	
Critical Maximum Redo Buffer Allocation Retry Rate	
Warning Maximum Redo Buffer Allocation Retry Rate	

C.9.13. Oracle::Table Extents

The Oracle::Table Extents probe monitors an Oracle database instance and collects the following metrics:

- Allocated Extents-Any Table — The total number of extents for any table.
- Available Extents-Any Table — The percentage of available extents for any table.

In Oracle, table extents allow a table to grow. When a table is full, it is *extended* by an amount of space

configured when the table is created. Extents are configured on a per-table basis, with an extent size and a maximum number of extents.

For example, a table that starts with 10 MB of space and that is configured with an extent size of 1 MB and max extents of 10 can grow to a maximum of 20 MB (by being extended by 1 MB ten times). This probe can be configured to alert by (1) the number of allocated extents (e.g. "go critical when the table has been extended 5 or more times"), or (2) the table is extended past a certain percentage of its max extents (e.g. "go critical when the table has exhausted 80% or more of its max extents").

The required **`Table Owner`** and **`Table Name`** fields contain a default value of **`%`** that matches any table owner or name.

Table C.60. Oracle::Table Extents settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Table Owner*	%
Table Name*	%
Timeout*	30
Critical Maximum Allocated Extents	
Warning Maximum Allocated Extents	
Critical Maximum Available Extents	
Warning Maximum Available Extents	

C.9.14. Oracle::Tablespace Usage

The Oracle::Tablespace Usage probe monitors an Oracle database instance and collects the following metric:

- Available Space Used — The percentage of available space in each tablespace that has been used.

Tablespace is the shared pool of space in which a set of tables live. This probe alerts the user when the total amount of available space falls below the threshold. Tablespace is measured in bytes, so extents do not factor into it directly (though each extension removes available space from the shared pool).

The required **`Tablespace Name`** field is case insensitive and contains a default value of **`%`** that matches any table name.

Table C.61. Oracle::Tablespace Usage settings

Field	Value
Oracle SID*	
Oracle Username*	
Oracle Password*	
Oracle Port*	1521
Tablespace Name*	%
Timeout*	30
Critical Maximum Available Space Used	
Warning Maximum Available Space Used	

C.9.15. Oracle::TNS Ping

The Oracle::TNS Ping probe determines if an Oracle listener is alive and collects the following metric:

- Remote Service Latency — The time it takes in seconds for the Oracle server to answer a connection request.

Table C.62. Oracle::TNS Ping settings

Field	Value
TNS Listener Port*	1521
Timeout*	15
Critical Maximum Remote Service Latency	
Warning Maximum Remote Service Latency	

C.10. RHN Satellite

The probes in this section may be applied to the RHN Satellite itself to monitor its health and performance. Since these probes run locally, no specific application or transport protocols are required.

C.10.1. RHN Satellite::Disk Space

The RHN Satellite::Disk Space probe monitors the free disk space on a Satellite and collects the following metrics:

- File System Used — The percent of the current file system now in use.
- Space Used — The file size used by the current file system.
- Space Available — The file size available to the current file system.

Table C.63. RHN Satellite::Disk Space settings

Field	Value
Device Pathname*	/dev/hda1
Critical Maximum File System Used	
Warning Maximum File System Used	
Critical Maximum Space Used	
Warning Maximum Space Used	
Critical Maximum Space Available	
Warning Maximum Space Available	

C.10.2. RHN Satellite::Execution Time

The RHN Satellite::Execution Time probe monitors the execution time for probes run from a Satellite and collects the following metric:

- Probe Execution Time Average — The seconds required to fully execute a probe.

Table C.64. RHN Satellite::Execution Time settings

Field	Value
Critical Maximum Probe Execution Time Average	
Warning Maximum Probe Execution Time Average	

C.10.3. RHN Satellite::Interface Traffic

The RHN Satellite::Interface Traffic probe monitors the interface traffic on a Satellite and collects the following metrics:

- Input Rate — The amount of traffic in bytes per second the device receives.
- Output Rate — The amount of traffic in bytes per second the device sends.

Table C.65. RHN Satellite::Interface Traffic settings

Field	Value
Interface*	eth0
Timeout (seconds)*	30
Critical Maximum Input Rate	
Critical Maximum Output Rate	

C.10.4. RHN Satellite::Latency

The RHN Satellite::Latency probe monitors the latency of probes on a Satellite and collects the following metric:

- Probe Latency Average — The lag in seconds between the time a probe becomes ready to run and the time it is actually run. Under normal conditions, this is generally less than a second. When a Satellite is overloaded (because it has too many probes with respect to their average execution time),

the number goes up.

Table C.66. RHN Satellite::Latency settings

Field	Value
Critical Maximum Probe Latency Average	
Warning Maximum Probe Latency Average	

C.10.5. RHN Satellite::Load

The RHN Satellite::Load probe monitors the CPU load on a Satellite and collects the following metric:

- Load — The load average on the CPU for a 1-, 5-, and 15-minute period.

Table C.67. RHN Satellite::Load settings

Field	Value
Critical Maximum 1-minute Average	
Warning Maximum 1-minute Average	
Critical Maximum 5-minute Average	
Warning Maximum 5-minute Average	
Critical Maximum 15-minute Average	
Warning Maximum 15-minute Average	

C.10.6. RHN Satellite::Probe Count

The RHN Satellite::Probe Count probe monitors the number of probes on a Satellite and collects the following metric:

- Probes — The number of individual probes running on a Satellite.

Table C.68. RHN Satellite::Probe Count settings

Field	Value
Critical Maximum Probe Count	
Warning Maximum Probe Count	

C.10.7. RHN Satellite::Process Counts

The RHN Satellite::Process Counts probe monitors the number of processes on a Satellite and collects the following metrics:

- Blocked — The number of processes that have been switched to the waiting queue and waiting state.
- Child — The number of processes spawned by another process already running on the machine.
- Defunct — The number of processes that have terminated (either because they have been killed by a signal or have called **`exit()`**) and whose parent processes have not yet received notification of their termination by executing some form of the **`wait()`** system call.

- Stopped — The number of processes that have stopped before their executions could be completed.
- Sleeping — A process that is in the **`Interruptible`** sleep state and that can later be reintroduced into memory, resuming execution where it left off.

Table C.69. RHN Satellite::Process Counts settings

Field	Value
Critical Maximum Blocked Processes	
Warning Maximum Blocked Processes	
Critical Maximum Child Processes	
Warning Maximum Child Processes	
Critical Maximum Defunct Processes	
Warning Maximum Defunct Processes	
Critical Maximum Stopped Processes	
Warning Maximum Stopped Processes	
Critical Maximum Sleeping Processes	
Warning Maximum Sleeping Processes	

C.10.8. RHN Satellite::Processes

The RHN Satellite::Processes probe monitors the number of processes on a Satellite and collects the following metric:

- Processes — The number of processes running simultaneously on the machine.

Table C.70. RHN Satellite::Processes settings

Field	Value
Critical Maximum Processes	
Warning Maximum Processes	

C.10.9. RHN Satellite::Process Health

The RHN Satellite::Process Health probe monitors customer-specified processes and collects the following metrics:

- CPU Usage — The CPU usage percent for a given process.
- Child Process Groups — The number of child processes spawned from the specified parent process. A child process inherits most of its attributes, such as open files, from its parent.
- Threads — The number of running threads for a given process. A thread is the basic unit of CPU utilization, and consists of a program counter, a register set, and a stack space. A thread is also called a lightweight process.
- Physical Memory Used — The amount of physical memory in kilobytes being used by the specified process.
- Virtual Memory Used — The amount of virtual memory in kilobytes being used by the specified process, or the size of the process in real memory plus swap.

Specify the process by its command name or process ID. (PID). Entering a PID overrides the entry of a

command name. If no command name or PID is entered, the error **`Command not found`** is displayed and the probe is set to a CRITICAL state.

Table C.71. RHN Satellite::Process Health settings

Field	Value
Command Name	
Process ID (PID) file	
Timeout*	15
Critical Maximum CPU Usage	
Warning Maximum CPU Usage	
Critical Maximum Child Process Groups	
Warning Maximum Child Process Groups	
Critical Maximum Threads	
Warning Maximum Threads	
Critical Maximum Physical Memory Used	
Warning Maximum Physical Memory Used	
Critical Maximum Virtual Memory Used	
Warning Maximum Virtual Memory Used	

C.10.10. RHN Satellite::Process Running

The RHN Satellite::Process Running probe verifies that the specified process is running. Specify the process by its command name or process ID. (PID). Entering a PID overrides the entry of a command name. A Critical status results if the probe cannot verify the command or PID.

Table C.72. RHN Satellite::Process Running settings

Field	Value
Command Name	
Process ID (PID) file	
Critical Number Running Maximum	
Critical Number Running Minimum	

C.10.11. RHN Satellite::Swap

The RHN Satellite::Swap probe monitors the percent of free swap space available on a Satellite. A CRITICAL status results if the value falls below the Critical threshold. A WARNING status results if the value falls below the Warning threshold.

Table C.73. RHN Satellite::Swap settings

Field	Value
Critical Minimum Swap Percent Free	
Warning Minimum Swap Percent Free	

C.10.12. RHN Satellite::Users

The RHN Satellite::Users probe monitors the number of users currently logged into a Satellite. A CRITICAL status results if the value exceeds the Critical threshold. A WARNING status results if the value exceeds the Warning threshold.

Table C.74. RHN Satellite::Users settings

Field	Value
Critical Maximum Users	
Warning Maximum Users	

Glossary

A

Action

A task that is scheduled by a system administrator using Red Hat Network to be performed on one or more client systems. For example, an action can be scheduled to update the kernel packages on all the systems within a selected group.

Activation Key

RHN Management and Provisioningcustomers can generate activation keys through the RHN website. Each unique key can then be used to register a Red Hat system, entitle the system to RHN, subscribe the system to specific channels, and subscribe the system to RHN system groups through the command line utility **`rhnreg_ks`** from the **`rhn_register`** package.

B

Base Channel

A base channel is a type of Channel that consists of a list of packages based on a specific architecture and Red Hat release. For example, all the packages in Red Hat Enterprise Linux AS 3 for the x86 architecture make a base channel.

Bug Fix Alert

An Errata Alert that pertains to a bug fix.

Bugzilla

Bugzilla is an online application (http://www.redhat.com/bugzilla) that allows users to communicate directly with the developers. From Bugzilla, users can submit bug reports and feature requests for Red Hat Enterprise Linux and related open source packages.

C

Channel

A channel is a list of packages. Channels are used to choose packages to be installed from client systems. Every client system must be subscribed to one Base Channel and can be subscribed to one or more Child Channel .

Child Channel

A child channel is a Channel associated with a Base Channel but contains extra packages.

Client System

See Registered System .

D

Digital Certificate

A client component in XML format that is stored in the **/etc/sysconfig/rhn/systemid** file on registered systems. Red Hat Network verifies this certificate to authenticate the registered system before each connection. This certificate is issued by Red Hat and passed to the system as part of the registration process. It includes unique information about the registered system to avoid fraudulent use.

E

Email Notification

Similar to an Errata Alert , except the information is delivered via email. If the email notifications option is selected, notifications are sent for every Red Hat Network Errata Alert . The email includes the type of Errata Alert, summary of the Errata, description of the Errata, and a list of which systems are affected by the report.

Enhancement Alert

An Errata Alert that pertains to a package enhancement request.

Entitled Server

A server that is subscribed to an RHN service level. Because the server is entitled, the RHN website can be used to manage its packages.

Errata

Information published by Red Hat describing security fixes, bug fixes, and package enhancements for Red Hat Enterprise Linux. The information includes the topics of the Errata, Bugzilla bug IDs, relevant releases/architectures, solutions including required RPMs, and MD5 checksums for verification. Errata are also available at http://www.redhat.com/errata/. Each RHN Errata Alert is based on the Red Hat Enterprise Linux Errata List.

Security issues and bug fixes are submitted by Red Hat engineers as well as the Linux community through Bugzilla which generates a bug report for each issue. Red Hat engineering evaluates the reports, resolves the bug, and generates new RPM packages. After the Red Hat

quality assurance team tests new packages they are placed on the Red Hat Public File Server and on the Red Hat Network Server and an Errata is generated.

Errata Alert

RHN Errata Alert that updated packages based on Red Hat Errata are available for one or more systems within an organization. There are three types of Errata Alerts: Security Alerts, Bug Fix Alerts, and Enhancement Alerts.

M

Management

One of the RHN service level offerings. It has more features than the Update service level, including user management, system groups, and enhanced system details.

N

Notification Method

An email address to which RHN Monitoring messages will be sent.

O

Organization Administrator

Organization Administrator are sets of users that have the highest level of control over an organization's Red Hat Network account. Members of this group can add users, systems, and system groups to the organization as well as remove them. An Organization Administrator can also give users administrative privileges to system groups. An RHN organization must have at least one member of the Organization Administrator group.

P

Package

All software in Red Hat Enterprise Linux is divided into software packages. Software updates are released in the form of RPM packages that can be installed on a Red Hat Enterprise Linux system.

Probe

A set of criteria that is either a template or a set of values assigned to a system that is used to measure the performance of a system.

Probe State

The measure of a probe's adherence to its defined criteria. States include: OK, Warning, Critical, Pending, Unknown

Probe Suite

collection or group of RHN Monitoring Probes.

Provisioning

One of the RHN service level offerings. It has more features than the Management service level, including kickstarting, reconfiguring, tracking, and reverting systems.

R

Red Hat Network Daemon

The RHN client daemon (**rhnsd**) that periodically polls Red Hat Network for scheduled actions.

Registered System

A system that is registered with Red Hat Network. Also known as a client system.

RPM

A software package manager that was developed by Red Hat Inc.. It can be used to build, install, query, verify, update, and uninstall software packages. All software updates from RHN are delivered in RPM format.

RPM Database

Each Red Hat Enterprise Linux system has an RPM database that stores information about all the RPM packages installed on the system. This information includes the version of the package, which files were installed with the package, a brief description of the package, the installation date, and more.

RPM Update

Red Hat Network option to deliver the RPM packages based on the Errata Alert list to a client system without user intervention. If this feature is selected, packages are delivered through the Red Hat Network Daemon running on the client system.

Red Hat Network Registration Client

The RHN client application (**rhn_register**) that collects information about the client system, creates a System Profile and Digital Certificate, establishes a connection with the Red Hat Network servers, and registers the system with Red Hat Network.

Red Hat Update Agent

The RHN client application (**up2date**) that allows users to retrieve and install all updated packages for the client system on which the application is run. Use the **Red Hat Update Agent Configuration Tool** to configure its preferences, including whether to install the packages after they are downloaded.

S

Security Alert

An Errata Alert that pertains to system security.

Service Level

A Red Hat Network subscription service. Different service levels offer different features of RHN. There are three paid service levels currently available: RHN Update, RHN Management, and RHN Provisioning.

Sibling

Siblings are virtual guests running on the same host. Virtual guests that run on separate hosts are not siblings.

Software Manager

The name of the first Service Level offering for Red Hat Network. Software Manager is now known as RHN Update .

System Directory

The System Directory section of Red Hat Network allows an organization to divide its client systems into system groups. Only members of the Organization Administrator group can add systems to the organization.

System ID

A unique string of characters and numbers that identifies a registered system. It is stored in the system's Digital Certificate .

System Profile

Hardware and software information about the client system. It is created during the registration process. The software information is a list of RPM packages and their versions installed on the client system. The System Profile is used to determine every Errata Alert relevant to each client system.

System Set Manager

Interface that allows users to perform actions on multiple systems. Actions include applying Errata Updates, upgrading packages, and adding/removing systems to/from system groups.

U

Update

One of the RHN service level offerings. Update was formerly called Basic. Update offers the same services as the Basic subscription did, plus more new features.

V

Virtual Guest

Any of the virtual instances running on the virtual host, under the control of the hypervisor. Also referred to as domain U or domU.

Virtual Host

The physical system that supports the hypervisor and all guest systems. The virtual host may also be referred to as domain 0, or dom0.

Y

Yellowdog Updater Modified (yum)

The Yellowdog Updater Modified is the Red Hat Network client application (**yum**) that allows users to retrieve and install new or updated packages for the client system on which the application is run.

Index

A

account
- deactivate, Account Deactivation

action
- completed systems, Action Details ⇒ Completed Systems
- details, Action Details ⇒ Details
- failed systems, Action Details ⇒ Failed Systems
- in progress systems, Action Details ⇒ In Progress Systems

activation key, Activation Keys —
- deleting, Managing Activation Keys
- disabling, Managing Activation Keys
- editing, Managing Activation Keys

activation keys
- creating, editing, and deleting, Managing Activation Keys
- multiple use, Using Multiple Activation Keys at Once —
- registration, Registering with Activation Keys
- using, Registering with Activation Keys

addresses
- change, Addresses

Apache
- probes, Apache 1.3.x and 2.0.x
- Processes, Apache::Processes
- Traffic, Apache::Traffic
- Uptime, Apache::Uptime

application programming interface
- API, RHN API Access

B

base channel, Software Channels

C

changing email address, User List ⇒ Active ⇒ User Details ⇒ Details —

changing password, User List ⇒ Active ⇒ User Details ⇒ Details —

Channel Entitlements, Channel Entitlements

Channel List , Software Channels

Channels
- Software and Configuration Files, Channels

channels, Channels
- all, All Channels
- base, Software Channels
- child, Software Channels
- entitling, Channel Entitlements
- errata, Software Channel Details ⇒ Errata
- list of, Software Channels
- packages, Software Channel Details ⇒ Packages
- relevant, Relevant Channels
- retired, Retired Channels

Channels and Packages
- Channel List, Software Channels

child channel, Software Channels

client applications
- obtaining, Before You Begin
- redirecting, Configuring the clients

client systems
- configuring, Configuring the clients

- registering, Registering Systems
- updating, Obtaining Updates

Config Channel List , Manage Config Channels —

config channels
- details, Configuration Channel Details ⇒ Details — , Configuration File Details ⇒ Details —
- global, Manage Config Channels ⇒ Config Channels —
- list of, Manage Config Channels —

Config Channels and Files
- Config Channel List, Manage Config Channels —

config management
- system preparation, Preparing Systems for Config Management

Configuration
- Channel List
  - Channel Details, Configuration Channel Details —
  - File Details, Configuration File Details —

configuration files
- manage, Manage Config Channels ⇒ Manage Files —
- quota, Manage Config Channels ⇒ Quota —

Configuration Management
- command line tools, Command Line Config Management Tools

custom information
- about systems, System Details ⇒ Details ⇒ Custom Info —

D

deactivate
- user, User List ⇒ Active ⇒ User Details —

delete
- user (RHN Satellite only), User List ⇒ Active ⇒ User Details —

deleting a system, System Details ⇒ Details

Digital Certificate, Security, Quality Assurance, and Red Hat Network

download ISO images, Download Software

E

email address
- change, Change Email
- changing, User List ⇒ Active ⇒ User Details ⇒ Details —

entitlement
- with activation key, Activation Keys —

entitlements
- purchase history, Expiration Dates &Purchase History

Errata, Errata
- Advanced Search, Advanced Search
- All Errata, All Errata
- apply applicable, System Details ⇒ Software ⇒ Errata
- Relevant Errata, Relevant Errata

Errata Alert Icons
- explanation of, Errata Alert Icons

Errata notifications
- automatic updates, Errata Notifications and Scheduled Package Installations

Errata Updates
- applying, Apply Errata Updates
- searching, Advanced Search
- viewing details, Errata Details
- viewing list of all errata, All Errata
- viewing list of applicable errata, Relevant Errata

G

General
- probes, General
- Remote Program, General::Remote Program
- Remote Program with Data, General::Remote Program with Data
- SNMP Check, General::SNMP Check
- TCP Check, General::TCP Check
- UDP Check, General::UDP Check
- Uptime (SNMP), General::Uptime (SNMP)

getting started, Before You Begin

GNU Privacy Guard, Security, Quality Assurance, and Red Hat Network

H

hardware profile
- Updating on server, System Details ⇒ Details ⇒ Hardware

Help Desk, Help

HTTP Proxy, Configuring the Applet

I

initialization script
- /etc/init.d/rhnsd , Red Hat Network Daemon
- /etc/rc.d/init.d/rhnsd , Red Hat Network Daemon

ISO images
- all, All ISOs
- download, Download Software
- relevant, Relevant ISOs

K

kickstart
- explained, Kickstart Explained

L

Linux
- CPU Usage, Linux::CPU Usage
- Disk IO Throughput, Linux::Disk IO Throughput
- Disk Usage, Linux::Disk Usage
- Inodes, Linux::Inodes
- Interface Traffic, Linux::Interface Traffic
- Load, Linux::Load
- Memory Usage, Linux::Memory Usage
- probes
  - nocpulse, Linux
- Process Count Total, Linux::Process Count Total
- Process Counts by State, Linux::Process Counts by State
- Process Health, Linux::Process Health
- Process Running, Linux::Process Running
- Swap Usage, Linux::Swap Usage
- TCP Connections by State, Linux::TCP Connections by State
- Users, Linux::Users
- Virtual Memory, Linux::Virtual Memory

List Navigation
- explanation of, Lists

LogAgent
- Log Pattern Match, LogAgent::Log Pattern Match
- Log Size, LogAgent::Log Size
- probes
  - nocpulse, LogAgent

M

macros
- within configuration Files
  - interpolation, Including Macros in your Configuration Files

Management
- service level, Management

manual installation
- System Profile, Manual Package Installation

Monitoring, Monitoring —
- All, Probe Status ⇒ All —
- Critical, Probe Status ⇒ Critical —
- Current State, Current State —
- General Config, General Config —
- introduction, Monitoring
- Notification, Notification —
- OK, Probe Status ⇒ OK —
- Pending, Probe Status ⇒ Pending —
- prerequisites, Prerequisites
- Scout Config Push, Scout Config Push —
- service level, Monitoring
- Status, Probe Status —
- Unknown, Probe Status ⇒ Unknown —
- Warning, Probe Status ⇒ Warning —

monitoring
- list of probes, Probes

MySQL , mysql-server package

- Database Accessibility, MySQL::Database Accessibility
- Open Tables, MySQL::Open Tables
- Opened Tables, MySQL::Opened Tables
- probes, MySQL 3.23 - 3.33
- Query Rate, MySQL::Query Rate
- Threads Running, MySQL::Threads Running

mysql-server package, mysql-server package

N

navigation, Navigation

Network Services
- DNS Lookup, Network Services::DNS Lookup
- FTP, Network Services::FTP
- IMAP Mail, Network Services::IMAP Mail
- Mail Transfer (SMTP), Network Services::Mail Transfer (SMTP)
- Ping, Network Services::Ping
- POP Mail, Network Services::POP Mail
- probes, Network Services
- Remote Ping, Network Services::Remote Ping
- RPCService, Network Services::RPCService
- Secure Web Server (HTTPS), Network Services::Secure Web Server (HTTPS)
- SSH, Network Services::SSH
- Web Server (HTTP), Network Services::Web Server (HTTP)

notes
- about systems, System Details ⇒ Details ⇒ Notes

Notification
- filter, General Config —

Notifications
- Monitoring, Notifications

notifications
- creating methods, Creating Notification Methods
- deleting methods, Deleting Notification Methods
- filtering, Filtering Notifications
- receiving, Receiving Notifications
- redirecting, Redirecting Notifications

ntsysv , Disabling

O

Oracle

- Active Sessions, Oracle::Active Sessions
- Availability, Oracle::Availability
- Blocking Sessions, Oracle::Blocking Sessions
- Buffer Cache, Oracle::Buffer Cache
- Client Connectivity, Oracle::Client Connectivity
- Data Dictionary Cache, Oracle::Data Dictionary Cache
- Disk Sort Ratio, Oracle::Disk Sort Ratio
- Idle Sessions, Oracle::Idle Sessions
- Index Extents, Oracle::Index Extents
- Library Cache, Oracle::Library Cache
- Locks, Oracle::Locks
- probes, Oracle 8i and 9i
- Redo Log, Oracle::Redo Log
- Table Extents, Oracle::Table Extents
- Tablespace Usage, Oracle::Tablespace Usage
- TNS Ping, Oracle::TNS Ping

Organization Administrator, User List ⇒ Active ⇒ User Details ⇒ Details —

overview of website, Categories and Pages

P

package installation
- scheduled, Errata Notifications and Scheduled Package Installations

package list
- Updating on server, Synchronizing Your System Profile, System Details ⇒ Software ⇒ Packages

packages
- filter, Software Channel Details ⇒ Packages

password
- change, Your Account

port 22, Configuring SSH

port 4545, Red Hat Network Monitoring Daemon (rhnmd)

preferences
- change, Your Preferences
- language, Locale Preferences
- locale, Locale Preferences

probe
- guidelines, Probe Guidelines

probe list

- Apache
  - Processes, Apache::Processes
  - Traffic, Apache::Traffic
  - Uptime, Apache::Uptime

- General
  - Remote Program, General::Remote Program
  - Remote Program with Data, General::Remote Program with Data
  - SNMP Check, General::SNMP Check
  - TCP Check, General::TCP Check
  - UDP Check, General::UDP Check
  - Uptime (SNMP), General::Uptime (SNMP)

- Linux
  - CPU Usage, Linux::CPU Usage
  - Disk IO Throughput, Linux::Disk IO Throughput
  - Disk Usage, Linux::Disk Usage
  - Inodes, Linux::Inodes
  - Interface Traffic, Linux::Interface Traffic
  - Load, Linux::Load
  - Memory Usage, Linux::Memory Usage
  - Process Count Total, Linux::Process Count Total
  - Process Counts by State, Linux::Process Counts by State
  - Process Health, Linux::Process Health
  - Process Running, Linux::Process Running
  - Swap Usage, Linux::Swap Usage
  - TCP Connections by State, Linux::TCP Connections by State
  - Users, Linux::Users
  - Virtual Memory, Linux::Virtual Memory

- LogAgent
  - Log Pattern Match, LogAgent::Log Pattern Match
  - Log Size, LogAgent::Log Size

- MySQL
  - Database Accessibility, MySQL::Database Accessibility
  - Open Tables, MySQL::Open Tables
  - Opened Tables, MySQL::Opened Tables
  - Query Rate, MySQL::Query Rate
  - Threads Running, MySQL::Threads Running

- Network Services
  - DNS Lookup, Network Services::DNS Lookup
  - FTP, Network Services::FTP
  - IMAP Mail, Network Services::IMAP Mail
  - Mail Transfer (SMTP), Network Services::Mail Transfer (SMTP)
  - Ping, Network Services::Ping
  - POP Mail, Network Services::POP Mail
  - Remote Ping, Network Services::Remote Ping

- RPCService, Network Services::RPCService
- Secure Web Server (HTTPS), Network Services::Secure Web Server (HTTPS)
- SSH, Network Services::SSH
- Web Server (HTTP), Network Services::Web Server (HTTP)

- Oracle
  - Active Sessions, Oracle::Active Sessions
  - Availability, Oracle::Availability
  - Blocking Sessions, Oracle::Blocking Sessions
  - Buffer Cache, Oracle::Buffer Cache
  - Client Connectivity, Oracle::Client Connectivity
  - Data Dictionary Cache, Oracle::Data Dictionary Cache
  - Disk Sort Ratio, Oracle::Disk Sort Ratio
  - Idle Sessions, Oracle::Idle Sessions
  - Index Extents, Oracle::Index Extents
  - Library Cache, Oracle::Library Cache
  - Locks, Oracle::Locks
  - Redo Log, Oracle::Redo Log
  - Table Extents, Oracle::Table Extents
  - Tablespace Usage, Oracle::Tablespace Usage
  - TNS Ping, Oracle::TNS Ping

- RHN Satellite
  - Disk Space, RHN Satellite::Disk Space
  - Execution Time, RHN Satellite::Execution Time
  - Interface Traffic, RHN Satellite::Interface Traffic
  - Latency, RHN Satellite::Latency
  - Load, RHN Satellite::Load
  - Probe Count, RHN Satellite::Probe Count
  - Process Counts, RHN Satellite::Process Counts
  - Process Health, RHN Satellite::Process Health
  - Process Running, RHN Satellite::Process Running
  - Processes, RHN Satellite::Processes
  - Swap, RHN Satellite::Swap
  - Users, RHN Satellite::Users

- WebLogic
  - Execute Queue, BEA WebLogic::Execute Queue
  - Heap Free, BEA WebLogic::Heap Free
  - JDBC Connection Pool, BEA WebLogic::JDBC Connection Pool
  - Server State, BEA WebLogic::Server State
  - Servlet, BEA WebLogic::Servlet

Probes

- Monitoring, Probes

probes

- Apache, Apache 1.3.x and 2.0.x
- General, General
- Linux, Linux
- LogAgent
    - nocpulse, LogAgent

- managing, Managing Probes
- MySQL, MySQL 3.23 - 3.33
- Network Services, Network Services
- on the RHN Server, Monitoring the RHN Server
- Oracle, Oracle 8i and 9i
- RHN Satellite, RHN Satellite
- thresholds, Establishing Thresholds
- WebLogic, BEA WebLogic 6.x and higher

Provisioning
- service level, Provisioning

proxy server
- with Red Hat Network Alert Notification Tool , Configuring the Applet
- with Red Hat Network Registration Client, Configuring the Red Hat Network Registration Client
- with Red Hat Update Agent, General Settings

Q

quality assurance
- overview, Security, Quality Assurance, and Red Hat Network

Quick Search
- explanation of, Quick Search

R

reactivating
- systems, System Details ⇒ Details ⇒ Reactivation —

Red Hat Enterprise Linux 2.1
- requiring the Red Hat Network Registration Client, Introduction to the Guide, Red Hat Update Agent

Red Hat Network
- an introduction to, Red Hat Network Overview
- components
    - primary, Red Hat Network Overview

Red Hat Network Actions Control
- rhn-actions-control , Red Hat Network Actions Control

Red Hat Network Alert Notification Tool
- adding to panel, Red Hat Network Alert Notification Tool
- applying Errata Updates, Applying Updates
- configuring, Configuring the Applet
- icons, Notification Icons
- launching RHN website, Launching the RHN Website
- requirements, Red Hat Network Alert Notification Tool
- with a proxy server, Configuring the Applet

Red Hat Network Configuration Client
- rhncfg-client , Red Hat Network Configuration Client

Red Hat Network Configuration Manager
- rhncfg-manager , Red Hat Network Configuration Manager

Red Hat Network Daemon, Red Hat Network Daemon
- configuring, Configuring
- disabling, Disabling
- initial description, Red Hat Network Overview
- troubleshooting, Troubleshooting
- using to apply Errata Updates, Apply Errata Updates
- viewing status, Viewing Status

Red Hat Network Monitoring Daemon
- (rhnmd) monitoring daemon, Red Hat Network Monitoring Daemon (rhnmd)
- installation, Installing the Red Hat Network Monitoring Daemon
- probes requiring the daemon, Probes requiring the daemon
- SSH key installation, Installing the SSH key
- using sshd instead, Configuring SSH

Red Hat Network packages
- comparison, Before You Begin

Red Hat Network Registration Client (rhn)_register)
- initial description, Red Hat Network Overview

Red Hat packages
- for UNIX, Download and Install Additional Packages

- installing, Download and Install Additional Packages

Red Hat Update Agent, Applying Updates
- Command Line Arguments, Command Line Version
- configuration, Configuration
- UNIX Command Line Arguments, Updating From the Command Line
- with a proxy server, General Settings

Red Hat Update Agent (up2date)
- activation keys, Registering with Activation Keys
- command line options, Command Line Version
- command line version, Command Line Version, Command Line Version
- configuration tool, Using the Red Hat Update Agent Configuration Tool
- configuring general settings, General Settings
- configuring package exceptions, Package Exceptions Settings
- configuring retrieval and installation, Retrieval/Installation Settings
- excluding packages, Package Exceptions Settings
- graphical options, Starting the Red Hat Update Agent
- initial description, Red Hat Network Overview
- installing GPG keys, Installing the Red Hat GPG key
- log file, Log File
- registering with, Registration
- starting, Starting the Red Hat Update Agent
- synchronizing system profile, Synchronizing Your System Profile

reference guide
- bug reporting, Send in Your Feedback
- conventions, Introduction to the Guide
- introduction to the, Introduction to the Guide

registering
- with activation keys, Registering with Activation Keys

Registration, Red Hat Network Registration Client
- as part of an organization, Registering a User Account
- Configuration, Configuring the Red Hat Network Registration Client
- Email notification, Registering a User Account
- Hardware System Profile, Hardware System Profile
- Password, Registering a User Account
- RPM Package List, Software System Profile
- Software System Profile, Software System Profile
- System Profile, Registering a User Account, Registering a System Profile
- text mode, Text Mode RHN Registration Client
- through the Web, Logging into the RHN Website
- username, Registering a User Account
- with a proxy server, Configuring the Red Hat Network Registration Client
- with activation key, Activation Keys —

remote commands
- enabling, Enabling Commands
- issuing, Issuing Commands

RHN Satellite
- Disk Space, RHN Satellite::Disk Space
- Execution Time, RHN Satellite::Execution Time
- Interface Traffic, RHN Satellite::Interface Traffic
- Latency, RHN Satellite::Latency
- Load, RHN Satellite::Load
- Probe Count, RHN Satellite::Probe Count
- probes, RHN Satellite
- Process Counts, RHN Satellite::Process Counts
- Process Health, RHN Satellite::Process Health
- Process Running, RHN Satellite::Process Running
- Processes, RHN Satellite::Processes
- Swap, RHN Satellite::Swap
- Users, RHN Satellite::Users

RHN Tools channel, Installing the Red Hat Network Monitoring Daemon

RHN website, Launching the RHN Website
- initial description, Red Hat Network Overview

rhn-catalog
- troubleshooting with, Examining Probes with rhn-catalog

rhn-runprobe
- options, Viewing the output of rhn-runprobe
- troubleshooting with, Viewing the output of rhn-runprobe

rhnmd daemon, Installing the Red Hat Network Monitoring Daemon

rhnreg_ks , Activation Keys —

rhnsd , Red Hat Network Daemon

rhn_register (see Registration)

RHUA; (up2date)
- complete description, Red Hat Update Agent

S

Schedule, Schedule

Scheduled Actions
- Action Details, Action Details
- Actions List, Actions List

- Archived Actions, Archived Actions
- Completed Actions, Completed Actions
- Failed Actions, Failed Actions
- Pending Actions, Pending Actions

Scout Config Push , Monitoring

Secure Sockets Layer, Security, Quality Assurance, and Red Hat Network

security
- overview, Security, Quality Assurance, and Red Hat Network

service levels
- Management, Management
- Monitoring, Monitoring
- Provisioning, Provisioning
- Update, Update

Software
- Channel List
  - Channel Details, Software Channel Details
- Package Search, Package Search

software
- searching, Package Search

software channels
- details, Software Channel Details ⇒ Details
- managers, Software Channel Details ⇒ Managers —
- subscribers, Software Channel Details ⇒ Subscribers —

SSH, Configuring SSH

SSH key, Installing the SSH key

sshd , Configuring SSH

SSL
- setting up, Configuring the clients

SSL certificates
- deploying, Deploying Client SSL Certificates

SSL expiration errors
- connection
  - certificate verification, Before You Begin

subscribe to channel, Software Channels

system group, System Groups —
- adding and removing, Adding and Removing Systems in Groups
- creating, Creating Groups
- deleting, System Group Details ⇒ Details —
- editing details, System Group Details ⇒ Details —
- list of, System Groups —
- viewing details, System Group Details —

system group list
- status, System Groups —

System Groups
- assigning and removing, System Details ⇒ Groups —
- System Group List, System Groups —

system groups
- joining and leaving, System Details ⇒ Groups —

system list, Systems

System Profile, Registering a System Profile
- Custom Information, System Details ⇒ Details ⇒ Custom Info —
- Notes, System Details ⇒ Details ⇒ Notes
- Reactivation, System Details ⇒ Details ⇒ Reactivation —
- Updating hardware profile, System Details ⇒ Details ⇒ Hardware
- Updating package list, Synchronizing Your System Profile, System Details ⇒ Software ⇒ Packages
- Updating Properties, System Details ⇒ Details ⇒ Properties

System Set Manager, System Set Manager —

systems
- deleting, System Details ⇒ Details
- entitling, Subscription Management
- overview, Overview —
- searching, Advanced Search —
- viewing a list of, Systems
- viewing details for, System Details

Systems
- Advanced Search, Advanced Search —
- Entitlements, Subscription Management
- System Details, System Details
- System List, Systems

- Systems Overview, Overview —

systems list
- status, Systems

Systems Selected
- explanation of, Systems Selected

T

Troubleshooting
- Monitoring, Troubleshooting

U

UNIX variants (see supported)

unsubscribe to channel, Software Channels

Update
- service level, Update

updating
- via command line, Updating From the Command Line
- via website, Updating Through the Website

user
- deactivate, User List ⇒ Active ⇒ User Details —
- delete (RHN Satellite only), User List ⇒ Active ⇒ User Details —

user account, Registering a User Account

user roles, User List ⇒ Active ⇒ User Details ⇒ Details —

users, Users —
- changing email address, User List ⇒ Active ⇒ User Details ⇒ Details —
- changing password, User List ⇒ Active ⇒ User Details ⇒ Details —
- roles, User List ⇒ Active ⇒ User Details ⇒ Details —

V

variables
- macros
  - in configuration files, Including Macros in your Configuration Files

W

WebLogic
- Execute Queue, BEA WebLogic::Execute Queue
- Heap Free, BEA WebLogic::Heap Free
- JDBC Connection Pool, BEA WebLogic::JDBC Connection Pool
- probes, BEA WebLogic 6.x and higher
- Server State, BEA WebLogic::Server State
- Servlet, BEA WebLogic::Servlet

website, Red Hat Network Website
- activation keys, Activation Keys —
- All Errata, All Errata
- Channel List, Software Channels
- Channels, Channels
- Config Channel List, Manage Config Channels —
- Configuration Channel Details, Configuration Channel Details —
- Configuration File Details, Configuration File Details —
- custom system information, Custom System Info —
- Errata, Errata
- Errata Search, Advanced Search
- Help, Help
- language, Locale Preferences
- locale, Locale Preferences
- logging in, Logging into the RHN Website
- Monitoring, Monitoring —
- navigation bar, Navigation
- overview, Navigation
- Purchase History, Expiration Dates &Purchase History
- Relevant Errata, Relevant Errata
- Schedule, Schedule
- Software Channel Details, Software Channel Details
- Software Search, Package Search
- stored profiles, Stored Profiles —
- System Details, System Details
- System Entitlements, Subscription Management
- System Group List, System Groups —
- System Groups, System Groups —
- System List, Systems
- System Search, Advanced Search —
- Systems, Systems
- Systems Overview, Overview —
- Users, Users —
- Your Account, Your Account
- Your RHN, Your RHN

Y

Your RHN, Your RHN
- Account Deactivation, Account Deactivation

- Addresses, Addresses
- Email, Change Email
- Help, Help
- Purchase History, Expiration Dates &Purchase History
- Your Account, Your Account
- Your Preferences, Your Preferences